



中国互联网法律 与政策研究报告 (2013)

 工业和信息化部电信研究院政策与经济研究所

 腾讯互联网与社会研究院

◎ 著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书全面梳理了国际上互联网领域的立法动态和趋势,介绍了2013年中国互联网领域的最新立法和政策,重点对2013年的互联网热点事件和近年来的主要司法案例进行了法律分析。本书对国际、国内互联网法律和政策进行了权威、系统、全面的解读,能够使读者对互联网法律和政策有全景式的了解,对互联网带来的最新法律问题有更深入的认识。

本书可供高等院校法学院师生、互联网公司从业人员和相关研究人员使用。

未经许可,不得以任何方式复制或抄袭本书的部分或全部内容。

版权所有,侵权必究。

图书在版编目(CIP)数据

中国互联网法律与政策研究报告.2013/工业和信息化部电信研究院政策与经济研究所,腾讯互联网与社会研究院著.一北京:电子工业出版社,2014.4

ISBN 978-7-121-22744-8

I. ①中… II. ①工… ②腾… III. ①互联网络—科学技术管理法规—研究报告—中国—2013 ②互联网络—科技政策—研究报告—中国—2013
IV. ①D922.174 ②F426.67

中国版本图书馆CIP数据核字(2014)第058290号

责任编辑:徐蔷薇

印 刷:三河市双峰印刷装订有限公司

装 订:三河市双峰印刷装订有限公司

出版发行:电子工业出版社

北京市海淀区万寿路173信箱 邮编 100036

开 本:720×1000 1/16 印张:20.5 字数:329千字

印 次:2014年4月第1次印刷

定 价:69.00元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010)88254888。

质量投诉请发邮件至zlt@phei.com.cn,盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线:(010)88258888。

《中国互联网法律与政策研究报告（2013）》

编 委 会

指导组

名誉顾问：曹淑敏 陈一丹 吴汉东 郭凯天

顾 问：刘 多 余晓晖 Brent Irvin

江 阳 谢 呼 江 波 刘 畅

主 任：鲁春丛 司 晓

成 员：辛勇飞 刘 勇 徐 炎 谢兰芳 王活涛 沈 丹

张 军 杜 军 朱劲松 杨 鹏 王小夏

编写组

主 任：马 源

副 主 任：李海英 张钦坤 赵 治

成员（按姓氏笔画排序）：

丁道勤 方 禹 王 融 田小军 石 月 冯明杰

卢鼎亮 伦 一 许长帅 曲柳莺 刘 彧 何华峰

李 丽 沈 玲 杨 乐 陈伟斯 杨筱敏 赵小彬

黄晓锦 龚 斌 彭宏洁 禄 源 谭 涛 蔡雄山

潘勤毅

序一

互联网已成为战略性公共基础设施，在我国经济发展、社会管理、公共服务、文化传播和对外开放中发挥着不可替代的作用。截至 2013 年年底，我国互联网宽带接入和移动互联网用户数均居全球首位；互联网服务收入近 6500 亿元，同比增长超过 40%；网络零售额突破 2 万亿元，6 年间增长 76 倍；政务微博与微信总数超过 10 万。互联网新技术、新业务的快速发展不仅推动了我国信息化进程，深刻影响了社会生产生活方式，也带来了管理、安全等方面的巨大挑战。互联网治理问题日益受到政府、产业和社会各界的普遍关注，依法治理互联网的需求也愈加迫切。

党的十八届三中全会明确提出了“推进法治中国建设”，建设法治中国，必须坚持依法治国、依法执政、依法行政共同推进，坚持法治国家、法治政府、法治社会一体建设。在互联网领域，依法治理需求更为突出。法律制度不仅是政府依法管理互联网的重要依据，也是实现互联网行业健康发展的重要保障。伴随互联网技术业务发展而产生的个人信息保护、垃圾信息治理、网络信息安全、网络知识产权保护、市场竞争秩序等一系列问题亟待通过法律制度予以明确和规范。

针对互联网发展和管理中产生的新问题，我国互联网法律制度体系正在初步构建，不仅包括对传统立法的修改，也包括针对互联网新属性、新问题的新立法。例如，2002 年 12 月 28 日，全国人民代表大会常务委员会出台了《全国人民代表大会常务委员会关于加强网络信息保护的決定》，以法律形式对解决互联网的突出问题作出了明确规定。但从整体上看，日新月异的互联网技术业务，仍然不断地向立法者、

执法者、互联网企业、用户等参与互联网的每个主体提出新的法律课题。

在此大背景下，及时总结我国互联网立法及司法领域取得的重大进展，关注国内外互联网立法动向与趋势，借鉴有益立法经验与科学制度具有十分重要的意义。本书的出版正是基于此目的，本书系统反映了工业和信息化部电信研究院和腾讯互联网与社会研究院的法律研究团队在互联网法律领域的研究成果，希望本书能够成为互联网企业、政府部门、立法机构、科研院所等关注互联网发展与管理的各界人士了解互联网法律与政策的窗口，为推进我国互联网法律体系的科学建设发挥积极作用。

工业和信息化部电信研究院院长 曹淑敏

2014年3月

序二

党的十八届三中全会对互联网的阐述再次证明，互联网已经成为我国经济创新发展的关键性基础设施，互联网经济已成为我国主体经济不可分割的一部分。经过 20 余年的发展，互联网已经并正在不断改变我们的生活、工作乃至思维方式。特别是最近几年，以移动化、社会化、本地化为特征的移动互联网，不仅将互联网应用载体从桌面延伸至智能终端，实现了互联网的泛在、无缝使用，并通过微信、O2O、基于位置服务、移动支付、手机娱乐等新模式赋予了互联网更新、更广的内涵和价值，促进信息消费稳步增长。

与 2000 年的互联网浪潮不同的是，3G/4G 网络、智能终端、云计算等的快速普及使得今天的互联网具备了参与或直接改变传统产业商业模式的能力。以零售业、金融、教育、房地产、旅游等为代表的传统产业都在积极地向互联网靠拢，一批富有活力的创造性新兴业态层出不穷。在这种浪潮中，互联网并非是对传统产业的破坏与颠覆，而是对传统产业薄弱环节的补充与加强。互联网金融的兴起就弥补了传统银行在资金处理效率、信息流整合方面的不足，有助于传统金融业创新服务模式与盈利模式。从这点来看，互联网与传统产业的跨界融合是应“时”发生，是用户和市场的选择，是合理存在的客观现象，符合国家提出的“使市场在资源配置中起决定性作用”的发展原则。从长远来看，互联网与传统产业相互渗透融合、相互促进，对传统产业降低成本、提高效率、改善服务、创新业态等方面有巨大作用。

诚然，任何一项创新业务在初始阶段都会有不确定性与风险，不完善之处在所难免。如果一味强调风险、安全，很有可能导致错失发

展的良机。此外，互联网具有零距离、全信息、去中心化、跨界性等有别于传统产业特征，任何违背其发展规律的管理方式都会阻碍行业发展。当前，互联网产业正处于创新密集期和关键转折点。随着新技术、新商业模式的融合，各种类似的互联网对传统产业的跨界创新会越来越多。这就需要业界各方预留一定时段的观察期，以发展为主题，以包容、试错的开放心态，集思广益，处理好创新和规范的关系，在发展过程中予以调整和完善，才能让这些新兴业态在健康的生态环境中稳定、快速地发展。

作为我国互联网行业发展的践行者，腾讯公司非常愿意与工业和信息化部电信研究院一道，在探索维护行业健康、有序发展的路径方面贡献自己的一份力量。为此，本书重点梳理了我国互联网领域的立法现状以及主要司法判例，深度分析了重大事件的起因和影响，总结了国外互联网立法和政策制定的经验，特别是融合背景下国外的主要做法。目的是以作他山之石，为推动我国互联网经济创新发展提供有益参考与借鉴。

腾讯公司高级副总裁 郭凯天

2014年3月

前言

2013 年，移动互联网向我们展开了宏大绚丽的图景。云计算、大数据发展如火如荼，互联网金融持续升温，微信迅速成为移动互联网的最热门应用之一。移动互联网的迅猛发展推动全球互联网进入了一个新的发展阶段。互联网立法作为互联网健康有序发展的规范保障，应适应互联网及社会发展需求，为互联网行业发展营造一个更好的法制环境。

国际方面，面对新技术、新业务的挑战，各国在政府数据开放、个人信息保护等方面提出了新的立法建议，以建立制度，着力提升关键基础设施的网络安全，探索传统反垄断规则在互联网领域的应用，同时在网络空间、网络犯罪、跨境数据流动等方面加强国际合作。

我国互联网法律制度自 20 世纪 90 年代以来经历了一个从无到有的建设过程。尤其是 2000 年以后，随着互联网逐步进入商用领域和实行市场化运作，我国有关互联网的立法活动也呈上升趋势，先后颁布了《全国人民代表大会常务委员会关于维护互联网安全的决定》、《互联网信息服务管理办法》等一系列法律规定。据初步统计，目前我国专门关于互联网的法律规定中，共有法律 3 部（其中两部为全国人民代表大会常务委员会发布的法律性文件），行政法规 6 部，部门规章 30 余部，司法解释 5 部。

2013 年，我国互联网立法主要集中于个人信息保护、电子商务等领域，同时，地方立法非常活跃，很多省份制定或出台了信息化条例，也在宽带建设、电子商务、个人信息保护等方面作了很多有益的探索。

本书共分五篇：国际篇、国内篇、区域篇、专题篇、案例篇，主要关注国际、国内互联网立法和政策的最新进展，对影响互联网发展的重大事件进行了法律分析，梳理了主要的互联网司法判例，同时收录了国家及地方层面的最新互联网立法摘编作为附录，以供读者查阅。本书由工业和信息化部电信研究院政策与经济研究所、腾讯互联网与社会研究院的法律研究团队共同撰写完成。在本书撰写过程中，得到了双方领导的大力支持和业内多位知名专家的指导与帮助，在此一并表示感谢。作为对 2013 年互联网法制建设的年度纪念，希望本书能够成为国内互联网法律领域具有学术深度和影响力的一本著作，为众多互联网从业者、研究者、关注者提供有价值的参考，书中疏漏与不足之处也请广大读者批评指正。

第一篇 国际篇

第一章 国际互联网立法发展概况	3
一、国际互联网立法概述	3
（一）互联网法律界定	3
（二）立法在互联网发展与管理中的作用	5
（三）互联网立法基本特点	6
（四）互联网立法主要领域	9
二、国际互联网立法最新趋势	27
（一）国家战略与立法提升关键基础设施安全保障水平	27
（二）大数据推动公共数据开放立法进程	29
（三）个人信息保护立法关注新技术、新业务	30
（四）网络版权立法尝试引入多样化执法手段	31
第二章 国际互联网立法热点	33
一、加快制定网络空间国际规则	33
（一）各国纷纷发布网络空间战略	34
（二）组建网络安全机构	34

(三) 网络犯罪国际治理部分达成一致	35
(四) 网络身份战略构建可信网络环境	35
二、加强网络与信息安全立法	36
(一) 关键 (信息) 基础设施立法活动在美国、欧盟、日本等 国家和地区全面铺开	36
(二) 信息安全战略陆续在欧盟、日本、俄罗斯出台	40
(三) 增设信息管理者责任以打击网络犯罪	42
(四) 开展互联网内容审查的国家不断增加	43
(五) “棱镜事件”迫使美国和英国立法机构作出调整	44
(六) 美 - 俄反恐双边协定中涵盖信息安全内容	47
三、多管齐下治理垃圾信息	48
(一) 通过立法完善垃圾信息管理制度	48
(二) 加强执法和制定监管政策, 实施垃圾信息治理	49
四、个人信息保护立法持续升温	50
(一) 欧委会推动欧盟个人数据保护立法重大改革	50
(二) 个人信息保护法的具体解释和执行规则进一步完善 ...	55
(三) 儿童等特殊敏感信息受到更为严格的法律保护	58
(四) 数据泄露通知制度被更广泛引入个人信息保护立法 ...	59
五、积极探索反垄断法适用互联网新规则	60
(一) 美国《横向合并指南》(2010年版)大大降低了 相关市场界定的重要性	60
(二) 欧盟采取相关市场界定与市场结构分析两种路径 判定互联网滥用市场支配地位的行为	61
(三) 互操作性、标准化和专利是当前互联网竞争行为 的重要特征	64

(四) 韩国积极探索竞争执法机构和行业监管机构之间的协调配合机制	65
第三章 国际互联网管理体制	66
一、多数国家未设立专门、统一的互联网管理机构	66
二、各国互联网管理机构的设置、职责一般以法律形式予以明确	67
三、设立互联网政策议事咨询机构, 提供政策发展建议	67
四、设立公共事业性机构, 协助政府促进业务开展	68
五、互联网网络安全机构所属类型多样	68
六、互联网内容管理机构行业化、民间化趋势逐步显现	69

第二篇 国内篇

第四章 我国互联网立法概述	73
一、我国互联网基础网络管理立法	73
二、我国互联网资源管理立法	74
三、我国互联网业务管理立法	74
四、我国互联网安全管理立法	75
第五章 我国互联网立法热点	76
一、我国个人信息保护立法取得重大进展	76
二、电子商务领域立法进程加快	79

(一) 2013 年电子商务领域出台的相关立法	79
(二) 电子商务领域相关立法起草工作取得积极进展	81
三、互联网市场竞争立法不断加强	83
四、网络版权保护力度进一步增强	84
(一) 通过修法加大法律惩处力度	84
(二) 行政执法持续打击网络侵权盗版行为	85
五、网络信息安全立法逐步启动	85
(一) 《关于加强移动智能终端管理的通知》	85
(二) 《关于办理利用信息网络实施诽谤等刑事案件 适用法律若干问题的解释》	87
第六章 2013 年主要宏观政策	89
一、大力发展信息消费	89
(一) 出台背景	89
(二) 政策概况	90
(三) 影响分析	91
二、发展宽带成为国家战略	91
(一) 出台背景	92
(二) 政策概况	93
(三) 影响分析	96
三、信息安全政策高端化和常态化	96
(一) 政策概况	96
(二) 影响分析	97
四、两化融合纵深推进	98
(一) 政策概况	98

(二) 影响分析	99
五、积极探索上海自贸区政策	100
(一) 出台背景	100
(二) 政策概况	101
(三) 影响分析	103

第三篇 区域篇

第七章 北京市	107
一、推动信息化条例出台	107
二、打击网络谣言	107
三、提高网络与信息安全事件突发应急能力	108
四、首提保护“网络安宁权”	108
五、加强舆论引导和互联网建设	109
六、确保互联网信息内容安全	110
第八章 上海市	111
一、推动信息化条例出台	111
二、促进电子商务发展	111
三、推动互联网基础网络建设	112
四、加强互联网新闻应急管理	112
五、拟立法推动网络个人信息保护	112

第九章 广东省	114
一、推动信息化条例出台	114
二、保障网络信息系统安全	114
三、维护互联网信息内容安全	115
四、推动电信基础设施建设	115
第十章 浙江省	116
一、推动信息化条例出台	116
二、加强通信计量监控	116
三、提升宽带网络服务质量	117
四、大力推进电子商务发展	117
第十一章 其他地区	119
一、湖南省出台全国首部信息化地方性法规	119
二、江苏省信息化条例明确规定个人信息保护	119
三、山西省信息化条例严惩出售个人隐私行为	120
四、海南省信息化条例强化信息网络和系统的监督管理	121
五、辽宁省修订计算机信息系统安全管理条例	121
六、重庆市推举措促消费增长	122
七、黑龙江省制定《移动智能终端服务公开承诺》	123
八、山东省全面推动网络经济发展	123
九、郑州市互联网业承诺保护公民个人隐私	124

第四篇 专题篇

第十二章 互联网金融创新..... 127

一、概述 127

二、法律分析 129

三、国外立法与借鉴..... 132

四、总结和评述 134

第十三章 “3·15 晚会”关注个人信息保护问题..... 135

一、概述 135

二、法律分析 135

三、国外立法与借鉴..... 137

 （一）“事先知情同意”（Prior Informed Consent）
 是关键 140

 （二）1995 年的数据保护指令仍然可以适用 140

 （三）浏览器许可（Browser Consent） 140

 （四）广告商和发行商的职责 140

四、总结和评述 142

第十四章 互联网市场竞争频现里程碑式案件 145

一、概述 145

 （一）腾讯诉奇虎不正当竞争纠纷案 145

 （二）百度诉奇虎 360 侵犯商标权及不正当竞争（插标行为
 与劫持流量行为） 147

(三) 百度诉奇虎 360 违反 Robots 协议不正当竞争	148
(四) 360 诉腾讯公司滥用市场支配地位纠纷案	149
二、法律分析	150
(一) 3Q 不正当竞争案中“360 隐私保护器”的监测 行为是否属于不正当竞争	150
(二) 3Q 不正当竞争案中的 360 扣扣保镖是否构成 不正当竞争	151
(三) 3B 不正当竞争案中的 Robots 协议是否具有 法律效力	152
(四) 3Q 垄断案中的相关产品市场如何界定	153
(五) 3Q 垄断案中腾讯公司在相关市场上是否具 有支配地位	154
三、国外立法与借鉴	155
(一) 关于不正当竞争	155
(二) 相关市场界定	156
(三) 市场支配地位认定	158
四、总结和评述	158
第十五章 “棱镜计划”引发全球关注	160
一、概述	160
二、法律分析	160
三、未来趋势	162
四、法律启示	163

第五篇 案例篇

第十六章 我国互联网相关司法案例概述.....	169
第十七章 典型法律问题分析	173
一、关于作品授权使用范围是否自动延及被授权方网络 平台的子域名系统.....	173
二、关于用户是否可以卸载、屏蔽互联网服务者提供 的广告等正当服务.....	175
三、关于搜索链接服务的免责边界问题	177
第十八章 典型案例判决要点	180
一、中国互联网新闻中心诉北京市盛世阳光文化传播有限 责任公司等侵犯著作权纠纷案.....	180
二、北京搜狐互联网信息服务有限公司等与乐视网信息技术 （北京）股份有限公司侵犯著作权系列纠纷案	181
三、北京搜狐新媒体信息技术有限公司诉北京风网信息技术 有限公司侵害作品信息网络传播权纠纷案.....	182
四、黄铁鹰等与合一信息技术（北京）有限公司侵害著作权 纠纷上诉案	183
五、谷歌公司（Google Inc.）与爱思美（北京）信息科技 有限公司著作权权属、侵权及不正当竞争纠纷上诉案.....	186

六、北京君和天下咨询有限公司诉北京掌中浩阅科技
有限公司侵害作品信息网络传播权纠纷案..... 189

七、北京百度网讯科技有限公司等诉北京奇虎科技
公司等侵犯商标权及不正当竞争纠纷案..... 190

八、腾讯科技（深圳）有限公司等诉北京奇虎科技
有限公司等不正当竞争纠纷案..... 198

九、袁腾飞诉北京多看科技有限公司侵犯信息网络
传播权纠纷案..... 204

十、北京奇虎科技有限公司诉腾讯科技（深圳）有限公司等
滥用市场支配地位纠纷案..... 205

附录

附录 A 国家层面立法摘编..... 213

附录 B 地方层面立法摘编..... 261

结束语..... 305

第一篇

国际篇



第一章 国际互联网立法发展概况

一、国际互联网立法概述

（一）互联网法律界定

随着互联网的快速发展及社会与经济影响力的不断上升，基于互联网的法律制度体系正在初步构建。互联网法律是指对通过互联网从事各种活动的自然人、法人和其他组织确定其权利、义务与责任，并调整各主体之间法律关系的规范总称。

1. 互联网法律的立法形式

从世界主要国家的立法实践看，规范和调整互联网行为或者活动的法律体现为两大类：一类是传统的、可直接适用于调整互联网相关活动的既有法律。虽然互联网具有虚拟性，但利用互联网从事活动的个人和组织却是真实存在的，互联网上的一些行为能够适用传统法律进行调整。例如，《刑法》或者《治安管理处罚法》可以同样追究通过互联网实施的违法犯罪活动的责任。另一类是专门规范互联网活动的法律规范。

互联网法律的立法形式有两种：一种是在传统法律基础上的修正与补充，以我国为例，近年来我国制定或修订的《国家安全法》、《著作权法》和《刑法》等，都补充和规定了一些与网络信息活动有密切关系的内容。另一种是制定全新的法律制度，例如，为遏制垃圾邮件的泛滥，美国、澳大利亚、日本、韩国等国家纷纷出台了反垃圾邮件法；为建立

网络平台上的商务活动规则，各国纷纷出台了《电子签名法》等电子商务法律；为加强保护网络环境下的个人信息，很多国家制定了《个人信息保护法》等。其中，针对互联网产生的特殊问题对传统法律规定进行修订或者补充，是互联网立法的常用形式。

2. 互联网法律的立法内容

综观世界主要国家的互联网法律，主要调整领域涉及网络犯罪、信息安全、电子商务、网上个人数据保护、网络著作权、垃圾邮件、互联网资源管理、互联网业务管理等方面。在内容方面，主要有如下两类法律规定。

一是从维护国家安全和社会公共利益出发，规定对互联网上的活动实施政府管理、对网络违法犯罪行为进行处罚或追究法律责任。我国有关互联网的大部分立法都属于这种情况，如《互联网信息服务管理办法》、《互联网新闻信息服务管理规定》、《全国人民代表大会常务委员会关于维护互联网安全的决定》等。另外，美国的《电子盗窃禁止法》、日本的《色情网站管制法》和韩国的《互联网内容过滤法令》，也属于这类法律。

二是从维护网络世界的正常秩序、保护网络参与方的合法权益出发，规定互联网活动参与各方的法律关系、权利和义务和法律后果。例如，美国《反网域名称抢注消费者保护法》规定，任何人不得将他人的注册商标抢先注册为域名。在涉及域名注册、交易或使用的民事（对人）诉讼中，法院可裁定没收或注销域名，或者责令将域名移转给商标权人。

当然，上述两类内容并非泾渭分明、非此即彼的关系，很多情况下可能同时并存。例如，我国《互联网电子邮件服务管理办法》既有要求互联网电子邮件服务提供者应当在电子邮件服务器开通前二十日将服务器所使用的 IP 地址向主管部门登记等行政管理的内容，同时也规范了互联网接入服务提供者、互联网电子邮件服务提供者和用户之

间的权利义务，如规定互联网电子邮件服务提供者对用户的个人注册信息和互联网电子邮件地址负有保密的义务等。

（二）立法在互联网发展与管理中的作用

无论是促进互联网的发展，还是实现互联网的有效管理，法律制度都是必不可少的。

在互联网发展方面，立法提供了切实的保障。例如，在法律层面降低互联网业务市场准入门槛，减轻管制负担，将大大促进互联网产业的市场活力；通过法律规定网络服务商在版权保护、处理违法不良信息方面的义务与责任，将减少服务商在经营中的法律风险。完善的法律制度对产业发展将起到明显的促进作用。

在互联网治理方面，经过多年的探索与实践，各国形成了以法律为基础，综合运用技术、经济、行政等多种手段的管理方式。在诸多方法和手段中，法律已成为规范互联网活动的前提和基础。无论是在管制较为宽松的英国，还是在管制较为严厉的新加坡，法律规定都是互联网运营和管理中不可缺少的部分。

从法律手段和其他手段在互联网管理活动中的运用来看，有三点需要说明。

第一，法律手段往往与其他手段同时运用。例如，美国在《未成年人互联网保护法》中明确规定：公立图书馆和学校的网络上必须安装过滤软件。上述规定以法律规范形式确认了技术手段的合法和正当性；美国《网络免税法》规定对自律性较好的企业给予优惠措施，属于经济调控手段的法律化；而我国大部分行政法律的主要内容之一，就是以法的形式确认政府的行政管理手段。

第二，并非所有的互联网上的活动都适合采用法律手段来调整。正如现实社会不能只靠法律来调整一样，网络社会也不能仅依靠法律

来调整。互联网活动中有的社会关系和社会行为本身不适合用法律来调整（如对用户正确使用互联网的教育、培训行为等），有的社会关系相比其他调整手段而言法律手段不是最佳选择。另外，互联网技术和应用日新月异的特点往往造成许多社会关系不适合通过具有相对稳定性的法律来调整。

第三，法律的有效执行需要其他手段的辅助。无论是国外还是国内，即便出台或修订了相关法律规定，其中的法律问题也难以马上解决，需要相应的法律辅助机制的配合。例如，在网络信息安全、网络知识产权、电子商务签名与认证问题方面，尽管相应的法律规定十分明确，但还有大量的违法行为存在。造成这种“令行禁不止”的原因很复杂，既与互联网本身非中心性、虚拟性、跨地域性和高度自治性关联，也产生于网上违法行为的隐蔽性、低成本和便捷性。因此，在看到法律作为互联网治理基础手段的同时，还应当建立一整套的法律辅助机制，包括技术手段、行政监督管理、信用体系等机制。

（三）互联网立法基本特点

尽管各国政治、经济、文化存在很大差异，但代表了互联网产业发展不同阶段，不同文化背景的美国、欧洲、日本、韩国、新加坡等国家和地区的互联网立法仍然体现出一些共性。

第一，互联网立法考虑互联网自身特殊属性。

互联网的跨国界性需要立法解决司法治权的问题。互联网作为连接全世界的通信工具，打破了地域、国界的限制，也直接挑战了国家的司法治权。解决互联网的问题，越来越需要国际合作。例如，欧盟制定的《网络犯罪公约》，除欧盟成员国之外，包括美国、日本等国家也成为签约国，这一公约是打击网络犯罪，构建统一法律框架的有益尝试。

互联网的灵活性需要具有相对稳定性的法律建立较为宽松的制度环境。互联网技术不断创新、互联网新业务层出不穷，法律应尽可能地不设立太多门槛与束缚，因为法律的稳定性会将束缚效应加以放大，影响技术创新与业务应用。美国、欧盟较早就通过法律取消了互联网业务的许可制度，并在很多法律或政策中贯彻“轻管制”原则。

互联网的开放性决定了立法是一个不断完善的过程。在开放的互联网环境下，任何人、任何群体都可以参与其中，法律作用的对象、领域变得如此之广泛。互联网的开放性决定了其立法进程将与现实社会的立法一样需要不断调整。自从互联网应用大规模普及以来，各国有关互联网的立法就没有停止过。

互联网的去中心化属性要求立法制度找到合理的规范切入点。互联网是网络的网络，价值链条越来越趋于扁平化，垂直的上下级的网络关系正趋于平行化。在规范对象方面，法律制度的选择要做得合理、科学才能保证管理的有效性。例如，在反垃圾邮件立法中，不但要规范邮件发送者、电子邮件服务提供者的行为，还要规范接入商的行为。

第二，互联网立法服务于国家互联网发展与管理思路。

互联网立法是促进互联网发展，实现有效管理的法律基础。立法活动应当首先符合国家层面对于互联网发展与管理的总体思路，以使各个互联网法律之间相互协调，总体目标一致。

在促进互联网发展方面，各国主要通过信息化战略，促进基础设施建设，提高互联网接入普及，推广互联网业务应用。欧盟“信息社会战略”明确了“技术中立”原则，因此，欧盟在法律层面建立了统一的“电子通信的管制框架”，适用于通过电子方式传输的通信服务，包括无线与固定，数据与语音，互联网与交换电路，广播业务和点到点的个人通信业务，消除了广播网络提供通信服务（例如，互联网接入、电话服务）以及电信运营商提供视听节目政策壁垒。韩国 IT839 战略

明确提出了互联网发展的各项具体指标，如对于 VOIP 业务，要求在 2010 年实现服务质量认可，因此韩国通信法中必须明确提供 VOIP 业务的各项技术要求。

在互联网管理思路方面，美国与欧盟都坚持“轻管制”原则。其中，美国关于互联网的管理思路清晰地体现在 1993 年和 1997 年克林顿 / 戈尔政府发布的《国家信息基础设施：行动计划》和《全球电子商务框架》两个文件中。在这两个文件中：

（1）确定了私营企业是互联网发展的主角。虽然美国政府已在资助 Internet 早期发展方面发挥了作用，但是 Internet 和 GII 的扩展主要由私营企业推动。

（2）强调了政府避免干预互联网的重要性。承认创新、丰富的服务、低廉的价格应该在一个竞争驱动的市场环境下产生，而不是在一个受管制的环境下产生。鼓励产业进行自我管制，支持私营企业开发能够促进互联网成功运作的机制。

（3）政府在其中所起的作用只是支持和加强一个可预测的、最简单的和前后一致的商业法制环境。

（4）在国际范围内促进 Internet 上的电子商务。承认各国法律制度各不相同，但是支持 Internet 上的商业交易和法律框架应当始终遵循与买卖双方所在国度无关的原则。

（5）保护知识产权。

（6）保障信息安全和网络可靠性。

以上思路对美国互联网立法产生了深刻的影响，法律文件所体现出的基本原则与思路基本相符合。因此，总体而言，互联网立法是国家贯彻互联网发展与管理思路的重要工具，立法要和国家战略所确立的发展与管理思路保持高度一致。

（四）互联网立法主要领域

1. 互联网内容管理立法

言论自由总是相对的。为保证公共利益，作为强大的内容传播平台的互联网无疑也需要管理。但在各国政治文化背景下，内容管理立法存在着多样性，例如，如何在尊重言论自由和尊重公共利益之间取得平衡？如何确定网络服务商、用户对于信息内容的管理责任？是否需要设立以及设立什么样的内容监管机构？如何区分内容管理的自律性义务和法定义务等？在对这些问题的处理上，各国立法各具特征。多数国家并没有通过法律对互联网信息（内容）服务设立市场准入门槛，但对于内容管理，各国仍显现出巨大差别。

1) 如何在尊重言论自由和尊重公共利益之间取得平衡

对于这一问题，崇尚言论自由的西方国家与注重社会秩序的东方国家有着显著的不同。美国是对内容管理较为宽松的国家，因为其一直严格秉承宪法第一修正案所确立的言论自由原则。美国内容管理的相关条款主要集中在儿童保护方面。《儿童互联网保护法》仅要求获得政府资助的公共图书馆和学校防止未成年人接入色情网站。

欧盟相对来说对内容管理也较为宽松，但因为欧盟非常注重文化多样性的问题，因此欧盟最新修订的《视听媒体服务无国界指令》在内容方面与美国相比有更多的规则，如要求所提供内容不包含种族歧视以及不恰当的有关性、宗教、国籍的内容；在业务经营中，注意推广欧盟的作品。

作为东方国家，新加坡与韩国在内容管理方面的法律十分全面与严格，包括服务提供商的登记制度，专门的内容管理机构，全面、细致的不良信息判断标准等。根据新加坡广播法，新加坡广播局需要保证互联网上的内容不违反公众利益、公共秩序与维护民众和睦的责任，

并保证其节目正派、有品位。禁止传播的内容包括违反公众利益、社会道德、公共秩序、社会安全、国家安定，或其他被新加坡适用法律禁止的内容。可见，东方国家对于内容管理更追究对社会秩序和公共利益的保护。

2) 如何规定网络服务商的内容管理责任

在内容管理中非常重要的一环是明确网络服务商的责任。明确服务商责任，有利于鼓励服务商及时报告不良信息，限制用户的恶意行为；也有利于减少服务商的法律风险，促进产业发展。目前，部分国家已出台相关内容管理法律。

美国法典第 42 章第 13032 节中规定了电子通信服务和远程计算机服务提供商关于儿童色情的报告义务，要求一旦知道存在儿童色情内容，就应该向国家儿童丢失及剥削中心报告。否则，将面临最高可达 10 万美元的罚款。法典第 42 章第 13031 节中规定了报告的格式，并规定了免责条款，报告人如果按照格式及时举报该内容，则不再担负民事或刑事责任。

日本《网络服务商责任法》明确规定：在互联网上出现诽谤中伤等信息时，若网络服务商应受害者的请求删除了这些信息，则免于承担对受害者的损害赔偿 responsibility。同时，网络服务商具有应受害方请求公示发信人信息的义务。

欧盟《电子商务指令》第 12 条至第 15 条对于特定情况下服务提供商的纯粹传输服务、缓存服务、宿主服务的责任作了限制性规定。

以上国家和地区对网络服务商的义务范围作了不同的规定，总体而言，欧盟的规定更加全面，给予网络服务商更多保护。

3) 采取怎样的内容管理模式

鉴于互联网传播信息的能力大大增强，在内容管理方面需要更快

的反应速度。因此，各国都建立了不良内容举报中心接受用户举报，并根据举报向相关网络服务商发出删除通知，及时消除不良影响，同时服务商保留相关记录，以备下一步的司法调查。例如，美国为严厉打击网上儿童性剥削行为，专门设立了报告机构——Cyber Tipline^①来负责接受告发；英国成立了互联网观察基金会，按照《3R 互联网安全规则》接受举报。

但由于政治文化背景的不同，在内容治理模式上东西方国家仍有差异。西方国家更多是“自治模式”，举报中心多由行业组织自发建立。东方国家更多为“共同治理”模式，强调政府的参与，例如，新加坡媒体发展局直接对 ICP 进行内容管制，包括发出删除通知；韩国信息通信部下设的互联网安全委员会在内容管理方面也拥有广泛的权力。

4) 如何在融合环境下考虑互联网内容管理

过去，内容管理是广播电视领域的工作重心。但随着广播电视、电信、互联网技术与业务的进一步融合，互联网已经能够传播过去只能在广播电视网上传输的视听媒体内容，互联网的媒体属性日益增强。

面对融合，各个国家和地区有不同的回应。新加坡将互联网看成一种媒体，适用于广播法的管理。而欧盟作出了新的创新，欧盟修改了其重要的内容管制指令《电视无国界指令》，将适用范围扩展到互联网，将管制对象区分为线形业务和非线形业务。线形业务指向传统电视、计算机、移动手机等终端定时的按照节目单传送的业务（Push Service），非线形业务指按照用户的需求传送的内容，如定制的电影或者新闻业务（Pull Service）。二者的区别在于前者用户的选择权和控制力相对较小，但对于社会的影响力较大。基于两种业务形态的差别，欧盟认为：对于非线形业务应当采取“轻管制”的思路，只需要符合一些基本规则，即指令 3c ~ 3h 条规定的内容，包括基本信息披露义务，

① 于 1998 年在联邦政府资助、国会授权的非政府组织 NCMEC 下建立。

所提供内容不对未成年人造成伤害；不包含种族歧视，不恰当的有关性、宗教、国籍的内容；在业务经营中，注意推广欧盟的作品等。非线性内容服务除了需要符合以上规定之外，不需要承担其他义务。

5) 如何设置内容监管机构

除了设立不良内容举报中心之外，对内容管理较为严格的国家还设有专门的监管部门。此外，考虑到互联网内容的多样性，同一个内容可能涉及传统的多个管理领域，内容属性的判定和划分较为复杂，因此，一些国家和地区通过设立统一的内容监管机构来实现有效管理。例如，新加坡设置了专门的内容管理机构——传媒发展管理局，依照统一的法规《分类许可制》和《互联网运行准则》对互联网信息内容实施监管；韩国成立了信息通信道德委员会（ICEC），作为互联网内容管理的专门机构，信息通信道德委员会的主要职责是评估涉及控制有害信息传播、促进更健康的网络文化发展的政策，其下设的专家委员会将针对未来可能出现的违法或有害信息的形式提出相关的鉴定标准等。

对于是否设立统一的内容监管部门这一问题，欧盟作出了较为弹性的规定。根据新修订的《视听媒体服务无国界指令》，欧盟认为成员国可以自行决定建立一个单一的视听媒体服务管制机构，也可以区分线形服务和非线性服务建立各自的监管机构，因为欧盟认为线形服务（广播服务）比非线性服务（点播服务）的影响力小，理应受到更为宽松的管理。

而在美国，并不存在内容管理的专门机构，更多的是依据传统法律进行事后处罚。例如，美国法典第 15 章第 52 条将传播虚假广告用于引诱或可能引诱购买食品、药物、设备、服务或化妆品的行为看成违法的，无论它通过何种方式传播。通过互联网传播虚假食品、药品信息的欺诈行为，由联邦贸易委员会（FTC）负责管理，FTC 是美国负责欺诈行为与反托拉斯的统一机构。

6) 内容分级与过滤

多数国家提倡内容分级与过滤的做法。美国提倡互联网服务提供商进行内容分级,并有专门机构提供内容分级系统;另外还有不同机构为家庭提供免费的内容过滤器。例如,设在美国的非营利性组织——家庭在线安全协会(FOSI)不仅为网站提供内容评级系统进行内容分级,还为家长免费提供内容过滤器,帮助他们防止自己的孩子访问不应该访问的内容;另外,一些州ISP协会也为家长免费提供内容过滤器。

韩国信息通信道德委员会引进了运营商及网民自愿性质的“互联网内容分级服务”。依据该服务,如果运营商已将其网站内容分级,则家长和老师可以通过一种特殊设计的软件搜索到合适级别的信息提供给青少年浏览,同时信息通信道德委员会也采取多种措施鼓励运营商对网站内容进行分级,并积极与有关部门加强合作。

7) 内容管理的其他方法

美国政府在内容管理方面能够采取的强制手段有限,其前后三次提出的有关内容管理的法案都被最高法院裁定为违宪。因此,美国政府更倚重于企业自律,为鼓励企业自律行为,美国在《互联网免税法》中规定,对于商业网站,如果网站向未成年人销售有害内容,将不能享受税收的豁免。这一做法有利于提高企业自律的积极性,提高自律效果。

2. 互联网资源管理立法

1) 各国立法概况

互联网资源主要指IP地址资源和域名资源。各国互联网资源管理的法律多集中于域名管理领域。例如,日本制定了《关于域名登记规则》,美国制定了《反抢注消费者保护法》,主要用于协调域名与商标权、名称权的法律关系。

在 IP 地址方面，则主要是一些分配政策。这主要是由于：IP 地址的分配管理主要由民间运作。美国 ICANN 是全球 IP 地址分配的最高机构，由其授权五大地区性机构再向下分配，这些机构根据 ICANN 的授权制定 IP 地址分配政策。这些政策不属于一国法律范畴。

2) 管理机构

（1）IP 地址分配管理机构。

在 ICANN 之下，IP 地址分配管理机构分为大区性分配管理机构（RIR）、国家级 IP 地址分配管理机构（NIR）和本地 IP 地址分配管理机构（LIR）。大区性 IP 地址分配管理机构目前包括 ARIN、APNIC 等五个得到 ICANN 认可的机构。国家级 IP 地址分配管理机构负责向本地 IP 地址分配管理机构分配 IP 地址，而本地 IP 地址分配管理机构一般为 ISP，它们向自己的网络用户或其他 ISP 分配 IP 地址。国家级 IP 地址分配管理机构通常存在于亚太地区国家。例如，中国、日本分别有 CNNIC 和 JPNIC，而美国并不存在这样一个机构，美国的大型 ISP 实际直接向大区性分配管理机构 ARIN 申请 IP 地址资源。

（2）域名管理机构。

各国在域名管理机构的设置上较为相似，基本采用了“域名注册管理机构—域名注册服务机构”的两级模式，由前者对后者实施指定授权、监督约束。采取这种机制可以创造公平竞争的域名注册服务市场环境，为域名申请者提供更好的服务，从而有利于域名的推广。

域名注册管理机构有营利和非营利两种类型。亚太国家以及欧盟的域名注册管理机构都不以营利为目的，而美国的域名注册管理机构 NeuStar 则是一个上市公司。但不管是否具有营利性质，这些机构与政府有着紧密的联系。承担韩国域名管理工作的机构互联网振兴院，由韩国电信监管机构 MIC 授权成立；日本 IP 地址管理机构日本网络信息中心（JPNIC）须接受总务省、经济产业省和文部科学省的监督。

NeuStar 根据与商务部签订的合同制定关于 .us 域名的具体管理政策。

3) 分配原则与收费制度

各国域名分配一般遵循“先到先得”原则。同时, 鉴于域名的商业价值, 以及为了促进域名的有效利用, 域名收费以成本为基础, 但也考虑市场的因素。各国分配域名时一般会收取一定的费用, 一般包括申请费和年费。日本规定, 域名等级不同申请费用不同, 美国规定按年收费, 收费的价格取决于被授权的注册机构及其转售渠道市场的定价。

IP 地址的收费原则有所不同, 基本上依据维护成本收费。如前文所述, 全球的 IP 资源由美国的 ICANN 机构统一分配, 同时又分别由大区、国家、本地管理机构协助分配。各大区在 IP 地址上的分配政策也并不相同。

有的大区分配机构采取会员制度。例如, 欧洲的大区机构 RIPE, 它的会员主要有欧洲的互联网服务提供商 (ISPS), 电信机构, 以及位于欧洲、中亚和中东的大公司, 会员可免费获得 IP 地址, 但是前提是运营商需要向本地互联网登记机构缴纳会费。

各国对 IP 地址的收费名目五花八门, 日本 JPNIC 向 IP 地址指定管理者收取的费用包括: 合同费、IP 地址维护费、IP 地址分配手续费等。美国、韩国的费用包括一次性费用及年费, 韩国的一次性费用叫“分担金”(相当于中国的担保金)。各国收取的费用差别也比较大, 韩国的担保金最多为 3000 美元, 而美国的一次性费用为 1250 ~ 18000 美元。

由于亚太地区初始获得的 IP 地址相对较少, 已经开始面临地址资源枯竭的问题。自 2007 年下半年起, 日本互联网信息中心 JPNIC 不定期发布《现有 IPv4 地址枯竭报告》。在这种情况下, 日本已经开始启用 IPv6 地址, 但 JPNIC 不负责 IPv6 地址的分配, IPv6 地址由申请人与 ISP 协商确定。日本使用 IPv4 和 IPv6 地址的费率不同, 具体费用根据 JPNIC 规定的《手续费规则》执行。

4) 域名注册管理制度

各国关于申请域名的条件规定集中体现地域原则。申请者必须为当地居民或者在当地有居所。

为了方便域名管理机构管理和建立域名数据库，获得域名的个人或企业一般应向管理域名分配机构履行登记手续。按照美国的有关规定，登记的信息包括注册人的物理通信地址、电子邮件、电话号码、首选域名服务器（Name Server）和备用域名服务器的 IP 地址、收费合同等。

5) 域名抢注问题

随着互联网商用化进程的不断加剧，域名被誉为企业的“网上商标”，因此，各国都很注重规范域名抢注问题，专门立法规范域名争端。从对恶意抢注行为的界定看，各国都非常重视保护已经享有“优先权”的权利人。例如，美国《反抢注消费者保护法》规定，赋予商标专有权人对域名本身的诉权，即商标专有权人不必分别针对各个域名抢注者提起诉讼，而是可以将侵犯商标专有权的域名的持有者一同诉诸法庭；同时还规定，授予商标专有权人对其被侵犯的域名，可以要求侵权人对其进行赔偿，赔偿数额或者按照实际损失或者按法定赔偿。

欧盟专门制定了受保护的域名列表，特别保护成员国的地理名称。此外，各国的域名管理机构都设立了域名注册争议的争端解决机制，但这些机构的裁决具有可诉性，即如果当事人对裁决不服，还可以向法院提出诉讼。

3. 垃圾信息立法

从国外立法看，大多数国家是针对垃圾信息进行统一立法，将电话、短信、邮件等形式的信息纳入一部立法进行规制。例如，欧盟、澳大利亚、日本、新加坡等国家和地区。

需要说明的是，由于垃圾信息最早期的形式是电话营销，因此一些发达国家，如美国最初是针对商业营销电话活动建立了“Do not Call”制度，但随着技术业务的发展，承载垃圾信息的渠道越来越多，除了电话以外，还有短信、邮件等方式，因此“Do not Call”制度所禁止的垃圾信息形式种类也在不断增加。例如，新加坡 2012 年《个人数据保护法》有专门的章节规定了“Do not Call”登记制度，该制度适用于通过所有方式发送消息，如语音呼叫、SMS、传真以及其他使用新加坡电话号码的数据发送应用程序，如“Whatsapp”，“iMessage”或者“Viber”等。

国外垃圾信息立法的主要内容如下。

（1）垃圾信息的范围。从各国立法来看，主要规范的是商业电子信息。各国立法对商业电子信息界定的共同特点是：

- ①其内容是推销产品或服务的商业广告或者商业、投资机会。
- ②其形式包括向移动电话发送的短信、互联网电子邮件和传真。

除了上述共同特点之外，各国对于垃圾信息的界定有其不尽一致的地方。新加坡的立法规定使用电话服务通过语音呼叫发送的信息不是电子信息。同时，商业电子信息的内容还包含帮助或者使人能够通过欺骗不诚实地获得他人的财产、金融利益等收益。澳大利亚的立法对商业电子信息内容的规定与新加坡类似。美国的 2003 年垃圾邮件法中明确规定垃圾邮件不仅包含商业电子邮件，还包含色情内容的邮件。

（2）各国对于商业电子邮件发送机制，在立法上有两种选择：一是“事前允诺”（opt-in），二是“事后退出”（opt-out）两种方式。“事前允诺”的规制方式是指邮件发送人向收信人发送商业邮件必须事前取得收信人的同意，否则即为违法；而“事后退出”的规制方式则是指发信人可以未经收信人事前同意或者要求而向其发送商业电子信息，

但是，如果收信人明确表明拒绝接收该类电子邮件，则不得再向该收信人发送相关邮件。

从各国立法来看，目前欧盟多数国家、澳大利亚、日本采取“事前允诺”的规制方式，美国、新加坡、中国香港地区则是采取“事后拒绝”的方式。

对于“opt-in”模式，在取得用户的明确同意方面，欧盟也规定了例外的情形，即企业可以向已经建立了商业关系的用户发送不请自来的通信。欧盟 2002 年《电子隐私指令》第 13 条第 2 款规定：“虽然有第 1 款之规定，按照 1995 年第 46 号 EC 指令，在销售某产品或业务时，自然人或法人可以使用从其客户处得到的电子联络详细资料直接营销其类似的产品或业务；只要在这些信息被收集后已明确地给用户机会以方便、免费的方式对这些电子联络详细资料的使用提出反对，或是就这些信息中的某条信息的使用其客户最初没有拒绝。”日本也有类似规定。

同样是“opt-in”模式的澳大利亚建立了“Do not Call”制度，由此既可以减缓法律的严苛而影响网络效应对广告宣传的积极作用，同时又能见有效地保护用户的权利。

对于实行“opt-out”原则的国家，如新加坡、美国和中国香港地区，也建立了“Do not Call”制度。

4. 网络版权立法

各国通过立法等手段对著作权进行保护，以促进科学、文化、艺术事业的发展、进步和繁荣。但是互联网的开放性和数字化媒介的发展使得作品的复制和传播有别于传统作品。两者的具体区别在于：一是形式和载体上的区别。传统作品附着于一定的有形媒体上，而在互联网环境下，任何作品都可以通过数字转换成二进制码进行存储和传播。二是在互联网环境下，作品的复制和传播成本很小，散播速度非

常快。但从本质上来说,两者并没有不同,都具备“独创性”和“可复制性”这两个要素。

网络环境下作品的高传播速度和低复制成本无疑给传统的著作权制度带来了严峻挑战。为此,需要建立起网络环境下的著作权保护制度,平衡创作者、传播者和使用者各方的利益,促进互联网及相关产业健康、有序的发展。

从美国、欧盟、日本、韩国几个国家和地区的立法情况看,美国、欧盟都制定了专门的版权保护法律,日本仍是沿用原有的传统立法,韩国则是对传统的著作权法进行了修订。

纵观各国立法,在关于网络环境下的版权保护立法中主要对以下几类问题进行了界定。

一是作品在网络传播过程中必将产生种种传输和存储行为,这些传输和存储行为是由于技术需要而必然产生的临时复制行为,那么如何认定这些行为的性质?从美国和欧盟的法律来看,都对仅提供服务平台的互联网服务提供商进行了免责。美国在《数字千年版权保护法》中给提供纯粹传输、缓存(Caching)、信息寄存(Residing)和信息定位(Location,相当于搜索功能)四类服务的互联网服务提供商提供了避风港。而欧盟的电子商务指令与2001/29/EC中,也作出了相关规定。例如,电子商务指令中,规定提供纯粹的传输服务、缓存服务和宿主(Hosting)服务的提供商不必对其提供服务的服务接受者的信息负责。在2001/29/EC中,也对给第三方之间提供作品网络传输服务的中介以免责。在美国和欧盟的立法中都规定了“通知-删除”机制,美国的“通知-删除”机制甚至并不是强制性的,只是期望互联网提供商作出上述行为。欧盟的电子商务指令中还明确了不应当要求服务提供者承担监督其传输和存储信息的一般性义务,也不应当要求服务提供者承担主动收集表明违法活动事实或情况的一般性义务。美国和欧盟上述法律规定反映了对互联网实施轻管制以及极力促进互联网发展的态度,

不希望通过过于严格的规定来阻碍互联网发展。

二是如何认定用户的独立复制行为的性质（不同于上述技术需要而引起的复制行为）？从美国和韩国的立法来看，他们都改变了传统版权法案的前提，即只是得到有版权的材料而没有滥用该材料进行获利也是违法的。例如，美国《数字千年版权保护法》规定未经允许在网上下载音乐、电影、游戏、软件等为非法行为；韩国也因为原有法律下，使用 P2P 下载 MP3 或电影的行为不能以侵犯著作权来进行处罚，而在 2005 年对著作权法重新进行了修订；欧盟对于用户的复制行为也作出了严格限定，要求必须是以版权所有者获得合理补偿为前提，自然人个人将复制品用于最终使用，不直接或间接用于赢利。

三是对直接侵犯网络著作权的行为作出了规定。从各国立法及实践来看，这些行为主要包括：①避开或破坏保护版权的技术措施，如美国和欧盟的立法规定；②制作、销售、散布用于非法复制作品的装置，如美国的立法规定以及日本的 Winny 案例。在 Winny 案例中，由于当事人开发和散布点对点网络文件交换软件，被京都地方法院以违反著作权法的罪名判处罚金 150 万日元（约合 1.28 万美元）。

版权保护制度是一把双刃剑，它在保护版权方创造热情的同时，也可能由于过度保护而阻碍知识的传播和产业的发展。这一方面要求立法上作出一些例外和变通，如欧盟对于公共图书馆、教育机构的非营利性复制行为给予了免责；另一方面也需要政府机构、相关产业、网络服务提供商携手合作，在打击违法盗版行为的同时，促进在线产业的繁荣发展，如欧委会牵头，联合电影产业、互联网服务提供商以及电信运营商促进在线电影的发展。

5. 电子商务立法

与传统商务活动相比，电子商务诸多环节需要以法律确定规则。传统商务活动在物理空间中展开，各国法律对于物理合同的基本要素、

要约、书面形式、签字盖章都有明确而具体的规定。但是当商务活动从物理空间转移到网络空间中进行时,交易主体、交易契约载体、交易空间的虚拟性使得传统法律对契约效力的规定无法适用于网络上的交易。如果法律不能明确解决以上问题,电子商务交易的基石将十分脆弱。

因此,围绕这些环节,电子商务立法包括三大组成部分:①确立电子签名的效力和使用规则,即制定《电子签名法》;②建立电子商务交易规则,即在很多国家体现为《电子合同法》;③建立与电子商务应用相配套的其他制度,如电子支付、电子商务税收等。针对前两个环节,各国陆续出台了相关法律,如美国的《全球和国内电子签名法》,韩国的《电子签名法》,新加坡的《电子交易法》,日本的《电子签名法》、《电子合同法》和《特别电子商务法》,欧盟的《电子签名指令》和《电子商务指令》。

从各国电子签名法的比较看,主要有以下特点。

一是明确什么样的电子签名、电子合同和电子记录具有与传统形式相同的法律效力和可执行力,这也是确立电子商务法律的前提。

二是规定电子签名的使用自主原则,注意消费者的权益保护,比较突出的如美国的《电子签名法》,其中就明确规定当事人是否采用电子签名应当由当事人自主决定,防止消费者因处于弱势地位而被迫采用电子手段从事交易。

三是表明对电子签名技术的使用态度。其中,美国、欧盟都持技术中立态度,不要求采用特定的电子签名技术。新加坡则有其自己的特点,它采用的是技术中立和特定技术相结合的折中办法,一方面,规定无论采用何种电子签名技术都具有法律效力;另一方面,又鼓励使用公认的实用的“安全电子签名”技术。这一做法在促进各种签名技术发展的同时,又具有现实中易于管理的意义。

四是确立电子签名的第三方认证机制。但是各国对第三方机构的准入机制和资质条件有不同规定。在第三方认证机构应当承担的责任限额上，各国也有不同看法。例如，欧盟明确规定电子签名服务者应该确保其所签发的证书内容的准确性。而新加坡立法则对认证机构的责任风险进行了限制，规定经政府管理机构许可的安全认证机构可以在其签发的电子凭证中说明其承担责任的限额。

五是规定了电子签名适用的例外。由于电子签名毕竟是一种较新的技术，在安全性、实际应用及与法律的衔接上有许多需要进一步完善的地方。如果让它完全取代传统签章，在实际应用中会带来高风险。因此，美国、欧盟、新加坡的立法中都规定了电子签名适用的例外，将一些仍不适宜通过网络传输的文件排除在外，使得法律对电子签名的认可有个循序渐进的过程。例如，美国法律中规定的例外包括继承关系、收养与婚姻关系的相关法律文件；司法文件；不动产交易与赠与合同；产权证书；授权委托书；商业票据；危害人们声明与健康的产品的交易、运输等。

在电子商务交易规则方面，日本、欧盟、美国的立法较为完善，主要体现了对消费者的保护。一方面，电子商务活动中，由于消费者与供应商之间缺乏直接的联系，因而透明度和信息披露对消费者而言非常重要。日本《特定电子商务法》要求经营者必须表明自己的真实、可靠身份。欧盟的规定则更加全面，信息披露要求包括：“身份信息、有关合同订立程序的信息（包括价格、产品服务）、个人数据处理的信息、供应商安全政策的信息、投诉程序的信息以及有关撤销权的信息”等。

另一方面，由于消费者在网上购物，易受到广告影响，容易出现冲动、草率的情形，出于保护消费者的目的，各国在不同程度上赋予了消费者不承担违约责任的撤销权。例如，日本在禁止经营者在网上不正当劝诱活动的同时，也特别规定为使消费者不因违反本人意愿签订的合同而造成损害，允许消费者在签约后一定期限（8日）内可无

条件解约。对于因消费者操作失误而产生的并非是消费者意愿的合同，消费者可以向经营者主张合同无效。由于网络环境下的虚拟性，为提高用户对电子商务的信任感，从法律上给予消费者更多保护，有利于促进电子商务的发展与普及。

对于网上税收等其他配套制度，总体上还处于研究探索阶段。

6. 个人信息保护立法

随着互联网和电子商务的日益普及，个人信息被滥用事件呈不断上升趋势，为了防止这一现象，各国纷纷立法保护个人信息。有些国家和地区颁布了《个人信息保护法》，如欧盟、日本和韩国。欧盟颁布的指令包括：1995年10月24日颁布的《关于个人数据处理和自由流动的个人保护指令》；1997年颁布的《电信领域的个人数据处理和隐私保护指令》，该指令要求电信服务提供商应保障网络安全以及用户的通信数据不被泄露；2002年7月12日发布的《在电子通信领域的个人数据处理和隐私保护指令》，这部指令将互联网数据纳入保护范围。在欧盟指令的指引下，欧洲各国近几年都颁布或修订了个人信息保护法。更多的国家虽然没有颁布专门的个人信息保护法，但却从保护个人隐私的角度立法，如美国颁布了《电子通信隐私法》及《儿童在线隐私保护法》。此外，有的国家还从行业准则、行业自律的角度加强个人信息保护，典型国家是美国。美国在个人数据保护方面倡导行业自律，其并没有在商业领域和公共服务领域进行全面的个人数据保护立法。同时，美国商务部1998年发布的《有效保护隐私权的自律规范》，就是一个要求美国网站从业者制定保护网络上个人资料与隐私权的自律规约。

从各国立法的内容来看，各国的个人信息保护制度具有以下几大特点。

（1）个人信息保护与隐私权的保护密不可分。这一点在美国最为突出，美国就没有制定专门的个人信息保护法，而是从保护隐私权的角度出发保护个人信息，这一点从相关立法的名称即可看出。美国作为世界上最推崇企业自律和创新的国家，对此有独到的政策取向，既要保护个人隐私权，同时又不阻碍信息的自由流动，从而推动电子商务和跨境交易。

（2）个人信息只可在合理的范围内收集和使用。日本《个人信息保护法》规定：个人信息尽量为特定目的使用；原则上禁止超范围使用个人信息；应恰当取得个人信息，在取得个人信息时通知使用目的等。韩国《2003年通信事业法》也规定：任何人从事通信服务时，不能利用工作之便破坏他人的通信秘密；检察院、军队、有关调查机关，或者其他为了维护国家安全的目的，需要运营商提供通信信息（包括姓名、身份证号码以及住址等）时，应当向运营商提供书面申请，申请内容包括原因、使用者、适用范围等（申请的相关内容法律另行规定），并且运营商应当对这些书面申请及所查询的资料依法存档；此外，《韩国公共机关个人信息保护法》规定，公共机关的负责人不得收集可能对思想、信条等个人的基本人权构成显著侵害的个人信息，除非取得信息主体同意或者其他法律规定可以收集；欧盟也有类似的规定。

（3）强调所提供的个人信息的准确性。日本《个人信息保护法》规定必须确保个人信息数据内容的正确性。欧盟在《电子通信领域的个人数据处理和隐私保护指令》中也规定，个人信息数据必须精确，而且如有必要必须及时更新；数据的实际控制者必须采取合理措施阻止错误数据，并保护数据不被修改、清除。

（4）对严重侵害个人信息的违法行为可能面临罚金，甚至监禁。日本《个人信息保护法》规定，如个人信息经营者违反主管大臣的命令，将受到严厉处罚，可能处以6个月以下监禁和30万日元以下罚金。同时，韩国《2003年电信事业法》第69条规定，违法泄露他人通信秘密；或

者违法向他人提供个人通信信息；或者违法获取通信信息的，可能判处 5000 万韩元的罚款或者 5 年以下监禁。

此外，比较特别的是，美国的相关立法尤其注重对儿童隐私权的保护，其 1998 年通过的《儿童在线隐私保护法》主要保护未成年人的个人信息，禁止网站从业者诱导未成年人填写个人信息，包括姓名、生日、住址、消费习惯、产品偏好，甚至父母年薪等资料。在许多情况下，一个网站要收集、披露和使用未成年人的个人信息必须获得其父母的同意。

7. 网络犯罪立法

网络犯罪并不是一个具体罪名，而是一类犯罪的总称。什么是网络犯罪，理论界有众多观点，比较主流的说法是：针对网络的犯罪和利用网络进行的犯罪。其具体表现形式包括：针对网络的犯罪如网络窃密，入侵、修改和删除计算机中的数据，制作、传播网络病毒，等等；利用网络进行的犯罪如网络盗窃，网络诈骗，网上色情，网上赌博，网上洗钱，网上贩卖违禁物品，信息污染（垃圾邮件、虚假信息等），版权盗版等。

从各国立法来看，由于犯罪行为的多样性，不可能由一部立法将所有的网络犯罪行为均吸纳进去，而是分别分布在传统立法及专门立法当中。例如，美国关于垃圾邮件的犯罪行为在 2003 年的《反垃圾邮件法》中得以规定，关于数字版权的犯罪行为在《数字千年版权保护法》中得到规定，关于对政府信息基础设施及金融基础设施的犯罪行为在《1996 年国家信息基础设施保护法》中进行了规定。日本政府自 2000 年起先后制定了多个专门针对网络犯罪的法律法规以及与其配套的对策措施，如《禁止非法链接法》、《色情网站管制法》等。

但是，各国立法当中也存在一个较相同的地方，就是对针对网络的犯罪进行了统一立法。例如，英国的《计算机濫用法》，美国 1984

年的《伪装进入设施和计算机欺诈及滥用法》和 1986 年的《计算机诈骗和滥用法》，新加坡的《防止滥用计算机法》，这些法律对于非法进入计算机网络获取材料（数据、程序），损坏计算机中的数据，故意干扰或阻碍计算机正常工作或禁止对计算机的访问，进入网络犯罪等滥用计算机的行为作出了限制。

各国立法的另一个特点是，网络犯罪的跨国界性使各国开始重视刑事政策和法律体系的协调与合作。传统的司法管辖权是以侵权行为地、住所地、国籍等属地为基础的，而网络的跨国界性，使得犯罪的行为发生地和结果发生地不具有同一性，从而打破了传统管辖权的属地确认原则。网络犯罪对传统司法管辖权的冲击需要各国之间相互协作，建立共同的刑法政策和法律体系，否则将无法对大量网络犯罪实施管辖。国际上对此已经有所行动，欧盟 2004 年生效的《网络犯罪公约》是打击网络犯罪的第一个国际公约，签署国除欧盟成员国之外，还包括美国、加拿大、日本、南非。该公约确立了网络犯罪的内容、刑罚、程序、司法监听和国际合作方面的共同框架，将有利于促进和协调世界各国在网络犯罪方面的刑事立法。

另外，由于网络犯罪是通过网络完成的，那么防护、打击与执法也必须在网络中完成。这就需要通过立法来确立执法机构对网络进行监听、巡逻、获取数据和要求相关服务商保存数据的权力。各国都对该方面的立法给予了重视，如美国 2002 年新修正的《网络安全加强法》，欧盟的《网络犯罪公约》，新加坡的《滥用计算机法》。

需要指出的是，对于网络犯罪的打击，一方面，需要有法律依据；另一方面，由于网络犯罪与传统犯罪相比，更具隐蔽性、取证更加困难，需要有相应的专门的网络犯罪管理体系才能有效打击网络犯罪行为。例如，美国从告发、调查到起诉已经形成了一套比较完善的体系。在告发环节上，不仅 FBI、密勤局等犯罪调查机构在各州设立了办事处，便于犯罪行为的告发，还专门设立了互联网犯罪投诉中心，在线接受

各个领域的网络犯罪投诉，并提交给相关调查机构。在调查环节上，有主要的调查机构 FBI 和美国密勤局，也有一些特殊部门的调查机构，如邮政检查局，移民和海关执行局等。在起诉环节上，美国 1995 年就已经针对网络犯罪和滥用知识产权犯罪建立了一套专门的公诉人体系，在每个检察官办公室指定一名或多名公诉人来负责网络犯罪案件的起诉。此后，美国又不断对该体系进行了完善。韩国警察厅在 2000 年也成立了网络犯罪应对中心，专门负责接受检举和调查，开发新技术和进行国际合作等打击网络犯罪的任务。

除了各国立法之外，互联网立法还有一部分体现在国际条约中，主要集中在数字版权、电子商务、网络犯罪三个领域。在数字版权领域，目前有《世界知识产权组织版权条约》和《世界知识产权组织表演和录音制品条约》，通常将这两部条约称为“国际互联网条约”，2002 年正式生效。在电子商务领域，主要有 1996 年联合国通过的《电子商务示范法》和《电子签名示范法》，2005 年的《联合国国际合同使用电子通信公约》。在网络犯罪领域，最主要的国际公约是 2001 年欧盟委员会通过的《网络犯罪公约》。

二、国际互联网立法最新趋势

（一）国家战略与立法提升关键基础设施安全保障水平

2013 年，随着信息技术的快速发展，网络安全事件频发，关键基础设施安全保障问题受到各国广泛关注，美国、欧盟、印度、俄罗斯等国家和地区都相继制定了国家层面的战略或出台了相关的法律法规，以提升关键基础设施安全保障的水平。美国 2013 年 2 月 12 日同时发布了一项行政命令（《促进关键基础设施网络安全的行政令》^①）和一

^① Improving Critical Infrastructure Cybersecurity.

项总统令（《保护关键基础设施之安全和可恢复的总统令》^①）；欧盟委员会 2013 年 2 月公布了“网络安全战略”^②，欧盟议会 2013 年 6 月通过了《“关键信息基础设施——面向全球网络安全”的决议》；印度政府 2013 年 5 月批准了《国家网络安全策略》^③，印度国家关键信息基础设施保护中心 2013 年 6 月发布了《保护国家关键信息基础设施指导原则》，此外，印度还准备针对关键基础设施安全保障实施专门的五年计划；俄罗斯联邦安全局 2013 年 8 月公布了《俄联邦关键网络基础设施安全》草案及修正案，拟于 2015 年 1 月 1 日由俄罗斯总统签署后予以实施。

从上述国家和地区针对关键基础设施安全保障的战略及立法来看，其核心内容集中在制度建设、信息共享和应急能力三个方面，呈现出一些特点：一是由战略指引向立法上升。例如，欧盟通过其“网络安全战略”提出了一项立法建议，有待下一步上升为欧盟指令——要求关键机构在遭受网络袭击时向欧盟汇报，包括重要基础设施的提供商、关键的网路企业及公共行政部门。二是重点关注关键基础设施安全保障的信息共享。信息共享是实现关键基础设施安全保障与多方快速协作的重要机制。各国信息共享机制主要包括三个层面，分别是政府部门与私营部门之间的信息共享，政府部门内部之间的信息共享，本国政府与外国政府之间的信息共享。三是针对应急反应能力提出专门要求。应急反应能力是应对关键基础设施安全威胁、恢复关键基础设施正常运营的关键要素，各国的战略及立法都予以提出了重点要求，包括建立国家级防护体系、建立应急反应机制、提升关键基础设施防护性能、制定应急响应计划或预案、提高应急反应情景意识等。

从当前趋势来看，未来世界各国对关键基础设施安全保护的关注

① Critical Infrastructure Security and Resilience.

② Cyber Security Strategy—An Open, Safe and Secure Cyberspace.

③ National Cyber Security Policy.

还会进一步加大，特别是在“棱镜门”事件发生后，承载重要信息的关键基础设施的安全问题将会得到前所未有的重视，各国都有决心从根本上提升关键基础设施的安全保障水平。

（二）大数据推动公共数据开放立法进程

大数据技术和业务的兴起，引发对数据开放的强烈需求，掌握重要数据资源的政府成为开放信息资源的带头人，各国积极通过法律和政策推动政府信息资源开放。

2013年6月，欧盟颁布对2003年《公共部门信息再利用指令》的修订指令（DIRECTIVE 2013/37/EU），要求公共部门提供透明、公平的信息再利用服务，扩大立法适用范围，将图书馆、博物馆和档案馆纳入。

2013年2月，美国科学技术政策办公室颁布《增加联邦资助的科研成果访问的政策》，让公众、产业界和科学界最大可能地访问联邦资助的科研成果。2013年5月，奥巴马颁布《政府信息公开和机器可读行政命令》：确保以多种方式让数据向公众发布，让数据易于被发现、获取和利用，政府部门应当保护个人隐私、保密和确保国家安全。

2013年6月，日本颁布《日本再兴战略》，提出开放数据，实现到2015年与其他发达国家同等水平的开放，出台个人数据处理方式的修订政策，促进公共数据向民间开放。

2013年7月，八国集团（美国、英国、法国、德国、意大利、加拿大、日本及俄罗斯）签署《开放数据宪章》。根据该宪章，英国、意大利、法国等国家都制定了开放数据的实施计划。

从各国立法的内容来看，主要确立了以下制度：

（1）政府默认数据开放。在政府数据开放的同时，遵守知识产权法、个人信息保护法和国家安全立法。

（2）确保数据开放的质量和数量。数据以最原始的状态开放，数据中包含的信息易于理解；尽早发布数据。

（3）数据被所有人使用。以开放的格式公开数据，释放尽可能多的数据，鼓励免费访问。公共部门应当提供透明、公平的信息再利用服务。

（4）开放数据，改善管理。各国间交流技术，保持数据采集、标准和程序透明。

（5）开放数据促进改革。鼓励应用程序开发者和社会组织参与促进数据开放的工作，鼓励下一代数据创新者提供数据的机器可读模式。

（三）个人信息保护立法关注新技术、新业务

当前，互联网新技术、新业务正前所未有地改变着个人信息的收集和使用方式，对现有的个人信息保护制度带来巨大挑战。云计算让个人信息远离个人终端，个人对于信息的控制能力逐步削弱；无处不在的移动互联网实时收集着高度个人化的信息；在社交网络上公开个人信息成为用户的日常行为；正在蓬勃兴起的大数据，能够通过数据关联和挖掘，轻而易举地重新恢复数据的身份属性。悄然变化着的网络世界和隐私观念正动摇着人们对于个人信息保护政策的信心。激进的观点认为：当前的网络环境下，隐私已经消亡，个人信息保护政策已到了退出历史舞台的时刻。

然而，从各国政策实践来看，个人信息保护政策非但没有消亡，其重要性反而得到提升。2012年1月25日，欧盟委员会发布了对《1995年数据保护指令》的改革建议，旨在在欧盟范围内建立更为统一和严格的立法，“棱镜计划”曝光后，立法进程大大加快。欧盟发布改革建议不到一个月，美国白宫也公布了隐私保护框架蓝图，呼吁国会制定消费者隐私权利保护法，这是美国政府第一次从联邦层面提出制定综

合性的隐私保护立法建议。该立法建议进一步明确了个人对于其信息的控制权利，同时美国政府也强调隐私立法将依然保持与商界和消费者团体的密切对话，更多地鼓励应用自律机制保护隐私。

作为对全球最有影响力的两种政策模式，欧美这两个相望于大西洋的政策主体在基本共识之外，对于个人信息保护政策的具体制度设计以及政策实施路径方面仍有很大差别，这些差别反映了二者对于个人信息保护政策基础理念的分歧。但是在经济全球一体化背景之下，欧盟和美国也无法忽略对方的利益诉求，在基本分歧之外，也有政策的相互妥协乃至彼此借鉴。例如，2012年的《欧盟个人数据保护立法建议》中借鉴了美国立法中开创的数据侵害事件通知制度：要求公司在数据侵害事件发生之后应当毫无延迟地通报监管机构，对于严重的的数据侵害事件，还应当通知受到影响的用户本人。同样，尽管美国对于欧盟此次立法改革中所提出的“遗忘权”诟病诸多，但也没有否认遗忘权对于某些需要重点保护的信息所具有的意义。美国加州近期出台法令，允许未成年人向互联网公司提出删除个人信息的要求，就是对欧盟提出的“遗忘权”的借鉴与改良。

（四）网络版权立法尝试引入多样化执法手段

互联网的迅猛发展对传统产业模式与规则形成巨大挑战与冲突，而部分国家也开始尝试在版权立法中引入多样化的执法手段，以更有力度地打击通过互联网实施的侵权行为。例如，美国国会曾推动出台《禁止网络盗版法案》（Stop Online Piracy Act, SOPA），该法律引入技术、经济、执法机制等综合手段，大大增强了知识产权的保护力度。其中，技术手段要求域名解析服务商、位置服务提供商、接入商停止对侵权网站的接入支持；经济手段要求位置服务商、广告服务提供商、金融服务商停止对侵权网站的商业和金融支持；执法机制则通过引入对物诉讼制度，使得美国司法机关对于美国境外的互联网站也能发起诉讼，

并配合以美国境内的执法活动最终停止其侵权活动。

法国在版权立法修改中提出“三振出局”制度，就侵权行为，依行为表现、情节轻重而采取不同程度的反击措施，对于网络侵权用户，经主管部门三次警告后，可以责令网络服务提供商中断网络服务，尽管此类法律制度仍面临较大争议，但尝试引入多样化的执法手段，不可否认地成为近年来互联网相关立法的显著特点。

第二章 国际互联网立法热点

一、加快制定网络空间国际规则

当前,互联网已深层次融入人类社会,网络空间已成为继领土、领海、领空、太空之后的第五空间和国家重要疆域,国际竞争日趋激烈。网络空间的国际规则成为亟待完善的领域,国际社会对于空间国际规则的制定一直处于不断完善与发展过程之中^①。近几年来,美国、欧盟、韩国、日本等发达国家和组织纷纷发布网络空间战略,阐述其网络空间的相关立场、主张及措施等。多数发展中国家也开始意识到网络空间国际规则的重要性,并加紧相关准备,规则的制定与掌控成为各方争夺焦点。

为了推动各方就网络空间国际规则达成一致共识,2011年11月1日至2日,首届“网络空间国际会议”(London International Conference on Cyberspace)在英国首都伦敦召开,这是国际社会各方首次就网络空间的经济、社会、犯罪、安全等问题展开的集中探讨。随后,2012年10月4日至5日,在匈牙利首都布达佩斯召开了第二次“网络空间国际会议”。此外,目前联合国信息安全专家组会议等继续研究信息和电信领域发展可能采取的合作措施,以应对现有和潜在的威胁。但目前相关会议仅是各方对网络空间国际规则的探讨,尚未形成有强制约束力的国际规则。

总体而言,相对于陆地、海洋、外层空间等传统空间,网络空间

^① 现代国际法规则已涉及人类所认识的所有自然空间。有关空间区域划分和相关法律规定分别体现在领土规则、海洋法、国际航空法、外层空间法等国际法分支中。

的国际规则正在形成过程之中。目前在网络资源、网络与信息安全、个人信息保护及网络犯罪等方面初步形成了以美欧为主导的部分规则，但在国际社会仍存在较大分歧。近年来，网络空间国际规则主要动向表现如下。

（一）各国纷纷发布网络空间战略

从2003年开始，美国相继发布了《网络空间国家战略》、《网络空间政策评估报告》、《网络空间可信身份标识战略》（2011）及《网络空间国际战略》（2011）。此后，欧盟成员国也陆续出台了相关网络安全战略，如德国的《信息基础设施保护国家计划》，瑞典的《改善瑞典网络安全战略》，爱沙尼亚在受到严重网络攻击后，于2008年发布了欧盟第一个广泛的国家层面的网络安全战略。目前，欧盟已有10个成员国发布了国家网络安全战略；一些成员国正在制定其网络安全战略，部分即将发布。此外，部分成员国有非官方或非正式的网络安全战略。2013年2月，欧盟委员会发布了第一个欧盟范围的《网络安全战略——一个开放、可信、安全的网络空间》。此外，韩国、日本等国也纷纷发布网络安全战略，阐述其网络空间的相关立场、主张及措施等。

（二）组建网络安全机构

各国在其网络安全战略或类似文件中大多组建了专门的网络安全机构，负责网络安全事宜。例如，日本网络空间战略的执行机构是内阁官房信息安全中心，该中心的上层领导是日本最高机构——IT战略本部（本部长为总理内阁大臣）和信息安全政策会议（议长为内阁官房长官）；韩国网络安全战略总体规划要求在国家网络安全中心（National Cyber Security Center, NCSC）^①下建立“国家网络威胁联合

^① 英文官网见：<http://service1.nis.go.kr/>。

响应团队”（National Cyber Threat Joint Response Team），由私人、公共及军事部门组成，以加强合作联系，如在参与部门间分享网络威胁信息；为防止网络攻击，维护网络安全，恢复受损网络，并在网络空间采取军事行动，2010年1月11日韩国国防部成立了网络战指挥中心（Cyberwarfare Command Center）等。此类机构的设立，目的在于加强网络安全监管，落实相应职责及采取相应网络安全措施。

（三）网络犯罪国际治理部分达成一致

目前，国际社会在网络犯罪国际治理方面达成了部分国际或区域性协议，但在实质性领域仍存在巨大差异。主要包括《布达佩斯公约》、《阿拉伯国家联盟打击信息技术犯罪法律框架》、《英联邦关于计算机和计算机犯罪示范法》、《上海合作组织国际信息安全领域的协议》等。

其中，影响较为广泛的是《布达佩斯公约》，全称为《网络犯罪公约》（Cyber-crime Convention），是2001年11月由欧洲理事会的26个欧盟成员国以及美国、加拿大、日本和南非等30个国家的政府官员在布达佩斯所共同签署的国际公约，是全世界第一部针对网络犯罪行为所制定的国际公约。遵循《网络犯罪公约》，能建立更广泛的共同打击网络犯罪的国际司法合作，对打击跨国网络犯罪具有重要作用。

（四）网络身份战略构建可信网络环境

在网络身份管理方面，许多国家已经启动或计划启动网络身份管理战略，且分别处于不同的阶段，如美国、澳大利亚、韩国等已经完成战略的制定，并正在实施当中。

目前，全球出现的网络身份管理典型模式主要有欧盟推行的电子身份证制度、韩国曾推行的网络实名制和美国推行的网络身份生

态系统三种。从国际经验来看，网络身份管理不仅可以在违法信息治理中发挥作用，其对经济和社会发展的影响更为深远。其中，战略顶层设计、技术实现路径、个人信息保护是有效实现网络身份管理的关键要素。

二、加强网络与信息安全立法

2013年，全球网络信息安全立法活动呈现出较为明显的“半年段”特征，以6月初爆发的“棱镜事件”为分水岭，上半年和下半年的立法热点明显不同，并呈现各自聚集化的特征。关键（信息）基础设施保护、网络信息安全战略、打击网络犯罪等领域的立法活动，大多于上半年完成；下半年，随着“棱镜事件”的爆发，包括美国、欧盟、澳大利亚、英国在内的众多国家和地区的立法机构都被迫停下原先设定的立法排期，临时加入众多与“棱镜事件”有关的法律议题，热点大多集中在本国原有的信息安全法律条文是否有效，如何对现有法律条文进行调整，或者出台新的法律草案等。相关立法热点如下。

（一）关键（信息）基础设施立法活动在美国、欧盟、日本等国家和地区全面铺开

2013年上半年，美国、欧盟在已有关键基础设施立法的基础上，继续完善相关立法。日本、印度等国家也开展相应立法。美国、欧盟、日本保持一致，将立法活动关注点都聚焦在关键（信息）基础设施的事前“安全性”和遭到攻击之后的“可恢复性”上；印度尚处于初级阶段，单纯将保障安全作为重点。

1. 美国

美国出台《保护关键基础设施之安全和可恢复的总统令》（以下简称《总统令》）和《促进关键基础设施之网络安全的行政令》（以下简

称《行政令》），其中对“关键基础设施”的定义源自《2001年爱国者法案》第1016(e)条。从目的上看，美国出台的这两份行政令，都是美国这十年间在关键基础设施保护上所遭受到的挫折、打击的总结；是对物理层面的设施和网络空间结合在一起之后风险效应乘数递增的意识；以及对百分之百地保障关键基础设施安全目标难度的承认，因此，《总统令》和《行政令》都很务实地将目标不仅定位于事前的“保护”，而是将事前的“保护”和受攻击之后的“可恢复”作为各占50%的目标。从内容上看，《总统令》的篇章布局分为“引言”、“政策”、“角色和职责”、“三大战略规则”、“创新、研究和发展”、“执行”、“关键基础设施之划定和部门职责”、“定义”八个部分，其中，将“关键基础设施”描述为设施实体、各类网络、各类系统三类，以及这三类事物的各种结合体。《行政令》的内容主要涵盖三个方面：网络安全信息共享；基于现有标准的风险操作系统；隐私和民权保护。另外，《行政令》将已经划定的16大关键基础设施的大部分保护职责都划分给了国土安全部。

★ 专栏：美国《保护关键基础设施之安全和可恢复的总统令》

2013年2月12日，白宫发布《保护关键基础设施之安全和可恢复的总统令》(PPD)，该《总统令》是对2003年《国土安全第七号总统令》的更新，主要是对新的危险环境的回应，以及这十年间在关键基础设施安全保护上美国对过去经验教训的总结，总体目标是修内功，重在提升自己的能力。

《总统令》发布的背景是：在美国，国家关键基础设施为美国提供了整个社会的基石。“关键基础设施”包括各类设施实体、各类网络、各类系统三大类，这些设施对于保持美国公民的信心，尤其是对于国家是安全的、繁荣的、有潜力创造诸多福利的公民信心。保护关键基础设施需要各方的共同合作，联邦、州、地方、部落及地区性实体，公共机构、私营部门，以及关键基础设施的拥有者、运营者应共同承担起各自的责任。

《总统令》的内容：提出三个事关这一目标全局的战略方向。其一，划定联邦政府部门之间在“关键基础设施”一事上的职责；其二，确保有效的信息交换，即设定联邦政府所需的最基础的数据和系统要求的相关信息；其

三，对于关键基础设施的计划和所有的运行决定，要将所有的各方信息综合起来看，并对其加以分析，以确定相关功能。

为达到目标，《总统令》提出6个步骤：一是120天内，划定国土安全部的职责，以及划定联邦政府其他机构的相关职责；二是150天内，对现有的公-私合作的机制进行评估，并提供评估结论和可选的改进方案；三是180天内，将提交给联邦政府的最基本的数据和系统信息进行验证，以确保未来相关信息交换的高效；四是240天内，打造一套关键基础设施形势预警系统；五是240天内，更新《国家基础设施保护计划》；六是2年内，完成一份《国家关键基础设施保护和可恢复性研究及相关发展计划》。

★ 专栏：美国《促进关键基础设施之网络安全的行政令》

《促进关键基础设施之网络安全的行政令》与上一专栏之《总统令》发布于同一天。《行政令》主要是联邦政府层级的各部门在保护网络关键基础设施安全方面的明确而详细的职责分工，并附有时间表。重要条文有：第四条“网络安全信息共享”，具体的细节由司法部部长、国土安全部部长和国家情报总监在120天内联合签署出台。第五条“隐私和民权保护”，赋予国土安全部一定的职责。第七条“减少对关键基础设施的网络威胁的基本框架”，规定商务部部长对NIST（国家标准和技术研究院）出台相关的框架予以负责。第八条“自愿性的关键基础设施网络安全项目”，主要是使得政府相关机构和基础设施的运营商、所有人（私营机构），以及其他对此事感兴趣的人，都能够参与到保护行动中来。第九条“处于最危险境地、风险最大的关键基础设施的认定”。150天之内，需要将这一类关键基础设施的范围确定。

总体上，《行政令》代表了美国在促进关键基础设施的网络安全保护方面，迈出了重要的、具有深远意义的一步。

2. 其他国家和地区

除美国之外，欧盟、印度、日本等国家及地区也各有动作。欧盟议会通过了《关键信息基础设施（CIIP）——面向全球网络安全的决议》，强调要加强ICT系统和网络应对各种破坏的可恢复性和安全能力，欧盟在整体层面做好准备，提高应对网络和信息基础设施安全挑战的技术能力。印度国家技术研究组织下设的国家关键信息基础设施保护

中心发布《保护国家关键信息基础设施指南》（以下简称《指南》），新提出 40 个具体的保护和控制措施，如识别关键基础设施、访问控制政策等。另外，《指南》也是对 2000 年印度《信息技术法案》中相关定义、政策内容的延续和拓展，印度政府自认为《指南》是达到全球先进标准的，虽然并没有提到关键基础设施受攻击之后的“可恢复性”。日本《重塑日本国家战略》正式出台，在“促进网络安全的措施”一节，提出为了应对打击、回应突发事件，要在重点的关键基础设施领域，加强网络安全手段建设，提升抗打击能力。此外，要尽快在全日本境内划定“重要关键基础设施”范围，在商业运营者和政府机构之间建立信息共享机制。

★ 专栏：欧盟《关键信息基础设施（CIIP）——面向全球网络安全的决议》

2013年6月12日，欧盟议会通过了《关键信息基础设施（CIIP）——面向全球网络安全的决议》，该决议大部分承认了欧盟委员会在2011年提出的建议。这些建议还被吸收到2013年出台的欧盟网络安全战略以及相关网络指令的内容中。本次有关CIIP的相关决议，承袭了上述欧盟关键基础设施保护政策的主要内容。

决议的几个重要方面是：建立欧盟成员国，以及欧洲公私机构有关网络恢复协作的欧洲论坛；执行泛欧行动（网络欧洲2010以及2012）；针对如何提高各成员国/政府计算机应急响应小组（CERTs）运作效率的问题，由欧洲网络与信息安全局（ENISA）制定对能力和服务的最低要求标准和相关的政策推荐。有关CIIP保护的要求将在未来的网络与信息安全指令中得到强化，该指令将会对成员国提出建立国家层面的安全保护以及与其他成员国进行协调合作的最低要求。

★ 专栏：印度《保护国家关键信息基础设施指南》

2013年6月，印度国家技术研究组织下设的国家关键信息基础设施保护中心的《保护国家关键信息基础设施指南》正式向公众公布。

该指导原则的第一版，原先是由国家安全顾问向总理提交的，而更加详细的版本，则是由“国家关键信息基础设施保护中心”（the National Critical

Information Infrastructure Protection Center, NCIIPC) 发布的。《指南》包括的关键信息基础设施的范围是:信息和通信、交通、能源、金融、技术、执法机构、安全机构、政府以及一些敏感的机构。

《指南》是对印度《IT ACT 2000》法案在法律意义上的延展,2000法案将“关键信息基础设施”定义为:“某些计算机资源的损毁,或者类似资源的归还,将对国家安全、经济、公众健康或者安全产生潜在影响。”

指导原则提出了40个控制措施,以保护关键信息基础设施,例如,识别关键信息基础设施,垂直和水平依存关系,信息安全部门,信息安全政策,培训和技能的提高,保护数据损失,访问控制政策等。

总体上,据印度自我评价(自我期望),该《指南》是达到“全球标准”的。

（二）信息安全战略陆续在欧盟、日本、俄罗斯出台

信息安全战略陆续在欧盟、日本和俄罗斯等国家和地区出台,其中,欧盟是出台单独的信息安全战略,俄罗斯和日本是在国家战略或者国家外交战略中涵盖信息安全战略。总体上看,各自定位不一,侧重点有别。

欧盟委员会通过《欧盟网络安全战略》,提出要在成员国之间建立统一的网络与信息安全标准,提高信任水平,促进欧盟内部统一市场进程。具体的手段是要引入一个“网络信息安全的最低标准”,在全欧境内促成标准的一致,以打击网络犯罪,并创造一个开放、安全的网络空间。俄罗斯《联邦外交政策理念》(以下简称《理念》)由普京签署,具有法律效力,与俄罗斯之前正式发布的一系列国家级文件文本相承接、相配套、相补充。《理念》中对信息安全的概念承袭了既往立场,与美国、欧盟等国家和地区提出的“网络自由化”、“网络透明”等针锋相对。主要内容涉及内容安全的重要性,本国政府对本国网络的绝对控制权,反对美国、英国等国提出的“网络自由化”、“网络无边界”等。日本在《重塑日本国家战略》中将“信息安全战略”纳入“促进网络安全的措施”一节,提出要将日本打造成为“全球最顶尖的IT社会”,为了尽快促成此目标,要继续打造全世界最坚韧、

最有力的网络空间，第一要务是提升网络空间安全的整体水平，具体措施包括：提升安全水平，打造政府机构的网络安全事件的应对体系，提升重要的关键基础设施的安全水平，发挥日本在促进国际网络空间安全战略和政策方面的积极作用。

★ 专栏：欧盟《欧盟网络安全战略》

2013年2月7日，欧委会提出了《欧盟网络安全战略》（以下简称《战略》）以及关于制定网络与信息安全指令的建议。《战略》和指令将在欧盟成员国之间建立更为统一的网络与信息安全标准，提高网络安全信任水平，促进欧盟内部统一市场进程。《战略》的初衷，是为了制定全欧范围内“网络与信息安

全”（NIS）的标准。《战略》的目的是通过引入NIS标准的最低要求（底线）来打击网络犯罪，创造一个开放、安全的网络空间。

《战略》出台的背景是：欧盟认为，当前网络安全事件的频率和影响广度都在增加，并对安全 and 经济造成了严重损害。欧盟的网络安全能力及成员国之间的协作水平亟待提升。据估计，在欧盟范围内每天大约有15万个电脑病毒在传播；根据世界经济论坛的统计，在未来10年，关键基础设施因遭受攻击而瘫痪的可能性已经上升到10%，二者将会造成大约2500亿美元的损失。另外，据2012年欧洲网络安全调查显示，大约38%的欧盟互联网用户出于网络安全担忧而改变行为习惯，18%的用户不愿使用网上银行业务；74%的受访者认为网络安全风险正在逐步增加，12%的受访者曾经历过网络诈骗。

《战略》的主要内容有：提出指导欧盟相关行动的基本原则和价值观，提升网络和信息系统的安

全和可恢复性，打击网络犯罪，部署网络防御，提出欧盟网络空间国际政策，明确欧盟、欧盟成员国以及相关机构的角色和责任。

此外，《战略》还明确将为提升成员国调查和打击网络犯罪能力提供帮助和支持，促进网络犯罪指令以及网络与信息安

★ 专栏：日本《重塑日本国家战略》

2013年6月14日，《重塑日本国家战略》（Japan Revitalization Strategy-Japan is BACK）正式出台，其中涵盖三个大的方略计划：一是产业重塑计划；二是

战略性的市场重塑计划；三是出口重塑计划。在第一大部分“产业重塑计划”中，其第四点是“将日本打造成为全世界最顶尖的IT社会”，内含6个行动方案，其中的第5个行动方案为“促进网络安全的措施”。

《战略》提出，要将日本打造成为“全球最顶尖的IT社会”，为了与该目标相适应，日本必须打造最坚韧、最有力的网络空间，要大力发展促进网络安全的各项措施，提升网络空间安全的整体水平，具体是：提升安全水平，政府机构的网络安全事件的应对体系，重要的关键基础设施的安全水平，以及发挥日本在促进国际网络空间安全战略和政策方面的积极作用。

（三）增设信息管理者责任以打击网络犯罪

欧盟议会通过《关于针对信息系统攻击的指令》（以下简称《指令》），主要涉及针对信息系统的大规模攻击的刑事犯罪的规制措施，总体上加大了对网络犯罪的处罚力度，并将一些新的行为纳入刑事法律的管制范围，例如，“利用软件实施大规模的攻击”，“使用复杂手段实施的攻击”以及“设计生产恶意软件”等行为都可以被作为刑事犯罪起诉追究；另外，《指令》规定了新的量刑加重情节以及更为严厉的刑罚制裁措施，如将监禁提高到至少两年；对于攻击国家信息基础设施的，诸如电力系统或者政府信息网络，将被处以5年监禁。此外，教唆、帮助、诱导此类犯罪也将被纳入刑事责任追究范围。澳大利亚司法部已向国会提交了《隐私法修正案》，作为对2012年《隐私法修正案》的再修正，本次主要是引入信息管理者在信息安全事故之后的强制通知制度（Mandatory Notification），也就是说，要求信息管理者在发生严重的数据泄露事故时，必须及时通知澳大利亚信息委员会和受影响用户。

★ 专栏：欧盟《关于针对信息系统攻击的指令》

2013年7月4日，欧盟议会表决通过了《关于针对信息系统攻击的指令》，由于该《指令》主要涉及针对信息系统的大规模攻击的刑事犯罪的规制措施，因此该《指令》的通过也被视为欧盟有关网络犯罪的重要立法动向。

《指令》的主要内容：《指令》在废除框架决议的同时，也保留了决议中的大部分条款，即对非法接入、非法的系统干扰、非法的数据干扰等行为的责任追究，并增加了新的条款（对以下两种行为予以刑事责任追究）：其一，使用各种手段（例如，病毒软件、僵尸网络或者非法获取的电脑密码）实施犯罪行为。其二，在犯罪活动中传授对信息系统的非法拦截方法。要加强现有的24×7（7天24小时）的联系点框架，要求各成员国响应点在8小时以内对紧急请求作出回复，收集有关网络犯罪的基础统计数据，通过以上行动提升欧盟打击网络犯罪过程中各机构之间的合作。此外，《指令》还将提高惩罚的严厉程度，如将监禁提高到至少两年；对于攻击国家信息基础设施的，如电力系统或者政府信息网络的，将被处以5年监禁。上述刑罚措施的严厉程度大大高于各成员国目前的量刑标准。此外，教唆、帮助、诱导此类犯罪也将被纳入责任追究体系。

（四）开展互联网内容审查的国家不断增加

随着互联网的日益普及和创新应用的日新月异，其带来的安全风险也日益增大，各国纷纷增强相关安全审查机制。从近两年的态势来看，主要表现在如下两个方面。

一是各国加强对内容层面的审查，开展互联网内容审查的国家不断增加。俄罗斯、英国、马来西亚、巴基斯坦、斯里兰卡等国家近两年相继加入互联网审查的国家行列，但各国的互联网内容审查范围会根据本国国情有所不同。例如，俄罗斯的互联网审查主要从保护青少年出发，根据其在2012年11月通过的相关法律，主要针对儿童色情、吸毒和自杀三种类型的不良违法内容。据报道，俄罗斯官方已经要求Facebook, Twitter和YouTube配合删除不良内容。由于网络色情影响不断扩大和恶化，英国首相卡梅伦2013年7月宣布政府将通过给用户设置过滤等措施打击网络色情，同时给搜索引擎公司施压，封堵那些可怕的色情关键词。马来西亚进行互联网内容审查是为了避免国内广大的穆斯林民众受到国外的不良影响。据报道，在2011年6月之前，马来西亚官方并不承认对互联网进行审查，尽管政府多次被谴责对某些

政治敏感网站进行了过滤。2011年6月，马来西亚多媒体通信委员会给所有马来西亚ISP发送了信函，声称违反了《1987年版权法》第41条，下令封锁一些网站，包括海盗湾（Pirate Bay）和几个文件托管网站，以及P2P通信。2013年5月13日，马来西亚政府大选，报道称国阵国民政府和民联政治领袖在Youtube和Facebook上的视频和网页被“封堵”。

二是各国担心设备给信息通信系统带来的安全风险，纷纷加强对设备的安全审查。2013年，美国国会通过的《2013财年综合继续拨款法案》，其中第516条对美国政府机构采购信息技术系统，特别是中国信息技术产品作出限制，要求商务部、司法部、国家空间宇航局、国家科学基金会采购信息技术系统之前，必须与联邦调查局及其他相关联邦机构一起对该系统所带来的网络间谍或网络破坏风险进行评估。印度自2010年以来，不断对各类电信业务许可协议进行修正，包括要求所有进口的信息和通信技术设备必须在印度境内的实验室进行检测；允许电信服务提供商和政府机构对设备商的制造设施和供应链进行检查；如果电信服务提供商的网络被检查出安全问题，电信设备商将被列入黑名单，设备将被拆除且不允许设备商再与电信服务提供商进行交易等。据报道，加拿大政府也在考虑是否修改移动运营商采购设备的法律法规来确保通信设备的安全。

（五）“棱镜事件”迫使美国和英国立法机构作出调整

“棱镜事件”爆发之后，在世界各国的一致声讨之下，美国和英国立法机构作出回应，主要是小范围削减情报机关权限，但情报机构、国家安全机关的监控实质和力度均未有改变。

2013年9月，美国国会召开棱镜情报系统改革听证会。这是棱镜事发3个月，美国立法机构首次正式的实质性回应。听证会围绕《情报控制和监控改革法案》（以下简称《法案》）的条文修正细节展开。

《法案》宗旨明确：保障美国公民的隐私权；调整棱镜实施机构——国家安全局和美国其他情报机构的监听、监控权限；调整监听、监控授权机构——外国情报监视法庭的职责。9月，英国议会情报和安全委员会对《调查权规范法案》和《情报服务法案》启动立法修正程序，重点围绕如何限制情报监听机构——英国政府通信总部的权限范围，以及对其使用监听权力进行程序上的规范。与美国类似，两部法案的修正都集中于国内机构权限和行动程序的调整，主要是为了回应本国民众的质疑。

★ 专栏：美国《情报控制和监控改革法案》

2013年9月26日，美国国会召开棱镜情报系统改革听证会。这是棱镜事发3个月，美国立法机构首次正式的实质性回应。听证会围绕《情报控制和监控改革法案》（The Intelligence Oversight and Surveillance Reform Act）的条文展开。这是“棱镜事件”被曝光之后，唯一一份由两党合作起草并临时排期、紧急加入国会立法议程的提案。《法案》的主要内容如下所述。

第一，对于电话记录数据：禁止国家安全局等情报执法机构大规模、 unlimited、无目标地收集美国公民的电话记录数据，无论这些美国公民是否有犯罪嫌疑。

鉴于电话监控的极端重要性，《法案》一旦通过，将砍去国家安全局的大半权力，并对美国情报系统的基石产生影响。今后，国家安全局再也不能拿着自己给自己颁发的临时强制令（而不是外国情报监视法庭的法庭准许令），私下找AT&T、Verizon要电话记录数据了。

当然，这一规定也有例外条款，即在恐怖袭击、外国间谍、核武器等紧急情况之下，国家安全局依然可以对本国民众“下手”，直接进行监控或者获取电话数据记录。但获取之后，应当在不超过7天的时间内拿到（补办）法庭准许令。

第二，对于互联网通信数据：禁止大规模收集网络数据。

9·11之后，凭借“反恐优先、隐私靠后”的国内政策和《爱国者法案》第215条，国家安全局曾经在一段时间内，大范围、大规模地收集美国公民的互联网通信数据，包括电子邮件、视频、网络电话，以及电子银行的用户名和密码。这一专门针对本国公民的大规模网络收集行动曾经在2010年被放弃，主要是因为数据实在是过于海量，并且有价值的不多，而情报机构又牵

扯了太多的精力在里面。但目前的法律条文的确是赋予了情报机构这样的权力，因此，从理论上来说，情报机构随时可以“卷土重来”。

本次的立法条文为竭力防止这种事情的发生，直接规定禁止国家安全局收集美国公民的互联网数据，除非有确凿证据证明有恐怖活动或者间谍嫌疑，或者是在紧急状态之下。

第三，对于搜索方式：堵住法律漏洞，禁止“后门搜索”和“反向搜索”。

FISA第702条授予国家安全局对外国目标（公民和机构）进行跟踪的权力。国家安全局在具体实行过程中，却经常不分国内、国外的目标和对象，借助对国外目标在跟踪过程中的数据搜索活动，一并对美国公民的信息进行搜索，即不分国内、国外地进行一揽子的跟踪和数据攫取。

本次的堵漏，主要是要堵住对美国本国公民的跟踪，要求国家安全局在搜索之前，先加入一个辨别程序，是“外国目标”，还是“美国公民”，还是“在美国境内的外国公民”。

堵漏针对两个目标：其一，“后门搜索”。以前国家安全局收集通信数据时，会对“相关的”的数据一起进行收集，例如，电子邮件的“发送人”、“收件人”、“抄送人”邮箱中的所有信息都在收集范围。其二，“反向收集”。由于对美国公民的数据进行收集，要事先拿到准许令，程序十分严格，国家安全局为了省略这些拿证的程序，先从有联系的外国目标开始跟踪，连带着把本国目标公民的数据也收集起来。今后，上述两种行为都要禁止。

第四，保护公司权益，含“受害”公司和“施害”公司。在立法机构看来，保住公司的权益，就等于保住了公司的信心，也就间接保住了普通民众对于互联网服务提供商的信心，将直接有益于互联网商业信心基石的重建。

公司在这里有两类：一是辅助国家安全局NSA实施“棱镜计划”的诸如Google、微软等大的跨国企业巨头，这些公司在“棱镜计划”中，扮演的是“辅助实施者”的角色；二是直接受到“棱镜计划”侵害的公司，这些公司的数据被NSA攫取，因而扮演的是“受害者”的角色。对于前一类公司，法律草案拟从“增加透明化”的角度予以帮助，即直接赋予这些公司以公布相关信息、数据的权利，例如，每年接到NSA多少次命令；交给NSA多少数据；关系到多少用户，到了什么程度，账号和密码是否一同交出等。对于后一类公司，赋予他们直接起诉的权利。

第五，改革中立监督机构——外国情报监视法庭。

作为为棱镜监控项目颁发法庭许可令的第三方司法机构，国会认为，该法庭在过去的这些年，根本没干什么有益的事情，对于国家安全局的数次申请，压根没有起到监督、防火墙的作用，而在某些方面，甚至对国家安全局等

情报机构私自扩大自身权限起到了推波助澜的作用，因此，在某种程度上，法庭的“不作为”是对FISA第702条的僭越，间接侵害了美国公民的宪法权利。

针对此，立法打算采用两个手段对该法庭进行监督：一是引入社会监督，以对该法庭起到制约和平衡的作用，目前，美国隐私和公民权利监督委员会已经入选；二是要求法庭每年向国会提交授权情报机构相关许可权限的年度报告。

★ 专栏：英国《调查权规范法案》（修正案）和《情报服务法案》（修正案）

2013年9月，英国议会情报和安全委员会正式对2000年《调查权规范法案》（The Regulation of Investigatory Powers Act, RIPA）和《情报服务法案》（the Intelligence Services Act）启动修正程序，内容如下：

对RIPA的修正，重点围绕的是如何限制GCHQ的权限范围，以及对GCHQ使用监听权力进行规范。例如，RIPA法案第8（4）款关于监听准许令的发放程序，将现有的一般情况下由英国国务大臣签署的程序基础上，加入法庭的签发程序。另外，紧急状况下该怎么签发监听准许令，目前还在商议过程中。另外的建议修正内容，主要涉及政府监听行动的相关信息公开化，例如，将以前政府对“国家安全威胁”一项的评估，由“中度”、“潜在”、“严重”的简单评估，改为由政府出台“国家安全威胁”的报告，一年一度向民众公布，包含的内容应该是花了多少钱、技术变化的影响、威胁次数、监控次数和范围等。

（六）美－俄反恐双边协定中涵盖信息安全内容

2013年6月，在北爱尔兰举办的“八国集团峰会”上，美－俄签署了一份关于联合反恐和联合遏制大规模杀伤性武器的双边协议，其中含有信息安全的相关内容。该协议规定，其签署的目的是，“出于国家安全之考虑，在应对网络信息安全事件时，需要实时沟通，最大限度地减少网络空间内的摩擦纠纷”。主要内容包括：两国在遇到或者可能遇到网络攻击时，要相互预警/警告；保持一个持续两年的沟通机制，尤其是关于那些重大的可能引发国家安全议题的网络攻击事

故，要加强沟通，增进两国在这一领域的相互理解；设立一个“热线”，在白宫网络信息安全协调官和俄罗斯同级官员之间，电话要能随时打得通。

三、多管齐下治理垃圾信息

（一）通过立法完善垃圾信息管理制度

2012年新加坡颁布《个人数据保护法》，建立了“不要呼叫”（Do not Call）登记制度。法律规定由个人数据保护委员会设立登记库，进行 Do not Call 登记。用户可以向委员会提交申请，将其电话号码在登记库中进行登记，经登记的号码不能再向该用户发送相关信息。法律作出了以下具体规定。

信息发送者的义务：任何人在发送信息之前，应当在规定的期限内向委员会提出申请，以确认电话号码是否在相关的登记中，如果没有，则可以发送。

如果用户或者电话号码使用者给予了明确和毫不含糊的同意接收指定消息，并且该同意可以通过书面形式或者其他形式证明，即使用户已经进行了电话登记，也可以成为发送者发送信息的抗辩理由。

对于发送信息的要求：

（1）指定消息包含明确的信息，以识别授权发送指定消息的个人或者组织；

（2）指定消息包含关于接收者可以容易地联系该发送者的明确的信息；

（3）指定消息包含的信息和遵循的条件应当符合管理规定；

（4）包含在指定消息中的信息在发送后的 30 天内是有效的。

（二）加强执法和制定监管政策，实施垃圾信息治理

韩国 KCC 不断升级减少垃圾邮件的措施：强化服务提供商自我管制；通过检查和改进每条传输线路的脆弱点来减少垃圾邮件的发送，通过增强实时的垃圾邮件处理能力来提高反垃圾邮件措施的效率。具体的措施包括以下四个方面：

- （1）移动电话反垃圾信息措施；
- （2）新的垃圾信息预防措施；
- （3）公布垃圾信息指数，提高垃圾信息处理基础，扩大国际合作；
- （4）提高用户对反垃圾信息的认识。

日本政府针对用户提出 3 条“安全对策”。据总务省《2011 信息通信白皮书》的介绍，垃圾邮件是日本互联网存在问题中占比最大的，2010 年达到了 34%，而且在移动互联方面，手机用户受垃圾邮件困扰的比例也是最大的，达到 29.7%。针对几乎令所有网民都很头疼的垃圾邮件问题，日本政府除严格实施《特定电子邮件正当发送法》等法律外，还通过开展普及网络安全教育，提出若干专门针对垃圾邮件的对策。日本政府针对网络用户提出的“安全对策”如下：

- （1）设置接收或拒绝邮件条件的接收限制；
- （2）使用提供商的垃圾邮件夹；
- （3）采取综合信息安全对策，使用处理垃圾邮件软件。

日本政府针对手机用户提出的“安全对策”如下：

- （1）使用长而复杂的邮件地址；
- （2）设置只接收指定域名和邮件地址发送的电子邮件；
- （3）慎重保存自己的邮件地址，不向无关人员透露。

四、个人信息保护立法持续升温

（一）欧委会推动欧盟个人数据保护立法重大改革

2012年1月25日，欧委会出台了《有关“涉及个人数据的处理及自由流动的个人数据保护指令（简称1995年数据保护指令）”的立法建议》，提出了个人数据保护立法一揽子改革计划。2013年6月，在“棱镜事件”曝光后，原本富有争议的欧盟个人数据保护立法改革进程大为加快。力倡立法改革的欧委会主席雷丁表示，“棱镜事件”为欧洲人敲响了警钟，包括德国总理默克尔在内的多位成员国首脑表示支持立法改革。2013年10月21日，欧洲议会公民自由委员会以绝对多数票通过立法提案。欧盟改革立法中引入的更为严格的数据保护制度让美国公司深感焦虑。新的立法规定：对于违反数据保护法律规定的行为，处罚将提升到公司全球年度收入的2%；超过250人的企业应设立“数据保护负责人”；明确引入“遗忘权”——当用户提出需求时，企业必须删除由其保存的个人数据。这些更为严格的制度将对美国互联网企业带来重大影响。美国互联网巨头，包括谷歌、亚马逊、脸书在内对此极为重视，派出游说人员在布鲁塞尔进行游说。欧洲议会目前已收到4400多份相关修正案意见，为欧盟立法修正案中最多，而其中大部分出自美国互联网企业的游说建议，这在欧盟立法史上也属罕见。

★ 专栏：欧盟《有关“涉及个人数据的处理及自由流动的个人数据保护指令（简称1995年数据保护指令）”的立法建议》

欧委会经过与利益相关方就现有个人数据保护法框架问题超过2年的密集咨询和研讨、一次2009年5月的高端会议，以及后续2个阶段的公众咨询程序后，2012年1月25日出台了《有关“涉及个人数据的处理及自由流动的个人数据保护指令（简称1995年数据保护指令）”的立法建议》（以下简称草案）。草案是为了对原有框架指令进行修订，以及提高欧盟现有立法的明确性，防止成员国执行的碎片化，以及防止用户丧失在线业务中个人数据得到保护的信心。

本草案的主要目的有两个：一是制定处理个人数据的规则，二是制定促进个人数据流动的规则。为出台该草案，欧委会执行了严格的影响评估程序，认为新草案将会大大提高欧盟个人数据保护水平。本草案包括6章共91条，结构上较原95指令更为合理和严谨，篇幅是原95指令的3倍。

背景和目的

欧盟关于个人数据保护的立法是95/46/EC指令^①，该指令从1995年开始实施，当时出于两个目的——保护个人数据涉及的基础性权利，保证成员国之间个人数据的自由流动。该指令在2008年被框架指令2008/977/JHA^②修订，补充了警察部门合作和刑事司法合作领域的个人数据保护的规则。此后，随着技术的快速发展，公私部门出于各自需要都开始大规模收集、共享个人数据。如果不更好地对个人数据进行保护，会打击用户使用在线业务的信心，会对整个社会发展不利。个人数据保护也是欧洲数字议程的中心任务。

新草案对于“基本权利”的概述

《欧盟基本权利宪章》第8条“将个人数据受保护权规定为基本权利”和《欧盟职能条约》(TFEU或《里斯本条约》)第16条(1)“确立的人人具有保护自身个人数据的原则”都是欧盟保护个人数据的法律权利基础。欧盟法院在2010年的多起案件判决意见中强调，保护个人数据的权利并不是一个绝对权，而是应当根据数据所产生的社会作用而定。个人数据保护与保护个人隐私及保护个人家庭生活权利密切相关，根据95/46/EC指令第1条(1)的规定，成员国应该保护个人基本的权利及自由，包括处理个人数据过程中涉及的个人隐私。欧盟法律规定的其他与个人数据保护权有关的基本权利包括言论表达自由、营业自由权，财产权特别是知识产权，禁止对诸如种族、民族、生理特征、宗教或信仰、政治观点、残疾、性别差异等方面的歧视，儿童受保护权，保持高水平健康状况权，信息公开权，受到有效法律救济或公平审判权。

① Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p.31.

② Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60 (“Framework Decision”).

新草案的修订或新增内容

（1）在“适用范围”条款里增加了不适用本指令的数据处理行为范围，即增加了“各成员国主管机构用于防止、调查、侦查刑事违法或执行刑罚过程中涉及的个人数据不适用于本指令”的规定。

适用对象方面，将《电子商务指令》（2000/31/EC）中“中间服务提供者”（纯粹传输服务提供者）处理个人数据的行为纳入本草案调整范围，意味着在线服务提供商在其服务过程中涉及信息的免责，不应突破个人数据保护的规定和要求。

（2）在定义条款里增加了新的法律概念，以扩充原95指令未涉及的相关内容。根据2002/58/EC指令和2009/136/EC指令，增加了“电子隐私”的概念。根据联合国《儿童权利和保护机构公约》的规定，增加了“基因数据”、“生物学数据”、“健康数据”，以及数据处理过程中涉及的“主营业”、“代表机构”、“企业”、“企事业团体”、“企业约束性行为规则”和“儿童”等概念。

修订了关于数据本人“同意”的概念，规定数据本人同意应当是本人明确的表达同意数据处理的口头、行为或书面的意思表示，更加清晰地界定了何为数据本人同意对其数据进行处理。

（3）对“合法处理个人数据原则”增加了“透明度原则”、“数据的最低程度说明义务原则”和“建立数据控制人的全面法律义务和责任原则”。同时对个人数据处理行为达到“合法处理的标准”又增加了利益平衡标准，即考察是否符合法律义务和公共利益。

（4）增加了在提供信息社会服务时，特别保护对儿童（即18以下未成年人）的个人数据处理的规则。

（5）规定数据控制人不能为执行本草案任何规定而额外收集用于识别数据本人的个人数据。

（6）在数据本人请求权规定方面，明确了数据控制人向数据本人提供数据的透明度义务，即采用简便和易于理解的数据提供方式；也考虑了互联网应用下，数据控制人向数据本人提供数据的特定程序和机制，如数据本人采用电子邮件等电子请求方式向数据控制人主张权利的情形、答复时限、答复要求等保护性规定。

增加了“共同数据控制人”、“共同数据处理人”等概念，明确共同行为和法律责任。

（7）进一步明确了数据控制人在数据处理过程中向数据本人通知的义务，除原95指令规定的“数据控制人、处理人身份”、“收集数据类型”、“数据处理目的”和“相关数据权利”外，增加了向数据本人告知“数据保存期

限”、“告知提起救济的方式”、“有关数据国际转移的事项”以及“数据来源（指数据控制人非直接从数据本人处获得数据的情况下）”的告知内容。

（8）在数据本人的数据修改、更正权的规定中，增加了数据遗忘权及其适用条件。

（9）针对云计算等新服务形式，增加了数据本人的“数据可携权”，即将数据从一个电子数据处理人处转移到另一电子数据处理人处，处理控制人无权干涉数据本人的此项权利。为了实现数据可携，数据控制人负有提供数据本人结构化及可兼容电子格式的数据等配合义务。

（10）在数据本人的拒绝权（拒绝数据控制人对其数据作出处理）方面，增加了数据本人在数据控制人因市场销售目的而处理其数据的拒绝权，以及该拒绝权排除适用的例外情形，即数据控制人履行证明责任，以及数据控制人能够证明其有合法排除数据本人拒绝权的合法理由。

（11）增加了一章关于“数据控制者和传输者”的规定，规定了两者在个人数据处理上的权利和义务，改变了原95指令单纯从数据本人角度设定法律权利义务的立法方式。这一改变，更好地规定了数据控制人、处理人的权利和义务，便于大众对法律规则的理解。在这一章也规定了数据控制人（处理人）的数据提供、更正义务，共同数据侵权责任（包括共同侵权的内部责任划分和对外责任），数据控制人（处理人）企业设立数据保护“代表”岗位的义务。

（12）简化了数据控制人（处理人）的事前报告义务，代之以自我约束的处理行为记录保存义务。改变了原95指令关于“数据处理前的数据控制人（处理人）向数据保护主管机构报告义务”的规定，改为数据控制人（处理人）自行保存其处理个人数据行为和过程的记录，在存在侵权隐患时应数据保护主管机构要求配合调查，查阅相关保存的行为记录。这一制度改变，有利于降低数据保护主管机构的行政成本和数据控制人的商业成本。

（13）在数据安全和保护责任上，要求即使未与数据本人订立合同，但是只要实际处理了个人数据，数据控制人（处理人）就有义务保护个人数据的安全。

（14）根据2002/58/EC指令关于电子隐私的数据侵权行为通知制度的规定，规定数据控制人（处理人）有向数据人履行“数据侵权发生的通知义务”。

（15）新增了数据控制人（处理人）开展数据保护效果评估和事前处理行为风险点评估义务。

（16）新增了在公共部门及大型私营企业或个人数据处理密集型企业设置信息保护官的规定，并规定了信息保护官的职责、权力履行方式。

（17）规定了欧委会可以通过规范个人数据处理的行为守则等法律文件，并考虑建立个人数据保护信任的认证机制或信任标志或信任商标。

（18）修订了“个人数据向第三国、国际组织转移”的规定，进一步明确了跨境和国际转移个人数据的基本规则，只要经欧委会认定该国或国际组织达到欧盟标准，向该国或组织转移个人数据就无须额外授权或认定。第一，明确了欧委会确定第三国个人数据保护欧盟标准的具体评估标准，包括第三国法律规定、司法救济及补偿水平和专门数据保护机构的设置等评估标准。第二，欧委会可以认定第三国、地区的某一行业或部门达到欧盟标准与否。第三，欧委会在向未达到保护标准的第三国和国际组织转移个人数据时，应向第三国或国际组织协商如何就被转移数据个人提供补偿的事宜。第四，在欧委会认定第三国未达到欧盟保护标准的情形下，采取其他的保护方式实现跨境数据转移，包括签订约束性商业行为规则或合同条款，在合同中设置专门的标准保护条款（由欧委会制定）、标准数据保护条款（成员国数据保护主管机构）。此外，欧委会或成员国数据保护主管机构可以确认相关合同及条款的合法性。对于如何理解和适用商业行为规则作出了具体规定。同时，对于何种情形下，数据转移须经数据本人的同意或授权作出了规定。第五，欧委会在欧盟官方公报上公布已达到其个人数据保护标准的第三国（部门、行业）名单。

（19）增加了成员国数据保护主管机构相互合作的义务。

（20）关于数据保护主管机构的管辖权协调问题。为解决不同成员国的管辖权重叠问题，建立了“一站式”管辖权原则，以保证草案的适用一致性问题。在数据控制人（处理人）在不同成员国都有营业机构的情况下，由数据控制人的“主营业”所在地的数据主管机构管辖该数据控制人在所有成员国内的数据处理行为。改变了原95指令关于数据处理行为发生地的数据主管机构管辖其地域范围内的数据处理行为的“分段式”管辖，部分解决了各成员国法律执行的碎片化问题。但强调各成员国法院排除数据主管机构的管辖权，仍根据各国司法管辖权范围执行本国关于个人数据保护的律。

（21）在授予各成员国数据主管机构的监督权问题上，增加了授予各成员国应当赋予其数据主管机构为履行职责，可以执行行政强制措施权力，扩大了数据主管机构履行职责的权利。

（22）增加了一章“合作及执行的一致性”的内容，专门调整各成员国数据保护主管机构的合作规则。第一，规定了强制性要求成员国数据主管机构多边合作的规则，包括信息请求、监管措施（包括数据处理前的审查授权措施等）、检查措施等，并且成员国数据主管机构相互请求的回复时限是1个月。第二，规定了成员国数据保护主管机构共同执行规则，包括联合开展调

查任务、联合采取执行措施等；在某一数据处理行为涉及多成员国时，主营业地数据主管机构可以请求有关成员国主管机构参与共同执法行动。第三，规定了各成员国数据主管机构采取的数据保护行为应当与委员会和欧盟数据保护委员会的要求一致，用欧盟数据保护委员会取代了原95指令设置的第29条工作组，由该委员确定关于向未达到欧盟数据保护标准的第三国转移个人数据的标准合同条款。第四，欧委会和欧盟数据保护委员会在成员国未协调执行本草案的问题上，要求成员国采取改正措施。

（23）扩充了原95指令关于“救济措施、法律责任和法律制裁”的规定。第一，明确行政救济权。规定除了数据本人之外，在数据侵权行为发生时，成员国内保护数据本人权益的团体、组织或机构（如消费者保护组织）可以代表本人利益向数据主管机构提起救济请求。第二，明确司法救济权。数据本人可以自由选择行政救济或司法救济。除由数据主管机构提供行政救济外，司法机关可以就数据控制人（处理人）侵犯数据本人的侵权行为进行司法救济。由数据控制人（处理人）所在地法院或数据本人住所地法院管辖。同时，为法院审查数据侵权案件规定了一些共同规则，包括用户保护机构或者成员国数据主管机构可以代替个人向法院提起诉讼，多个成员国法院同时管辖同一个侵权案件的“平行管辖”的处理。第三，明确司法监督权。规定公民或法人可以在成员国数据保护主管机构怠于履行职责时，向法院请求司法救济，成员国法院应当执行司法审查后的决定。第四，要求成员国对侵犯个人数据的行为设置刑罚惩罚和行政制裁措施，为行政制裁措施规定了个案最高额罚金限制等。

（24）在“特殊个人数据处理的义务豁免”规定方面，进一步增加了为保证公共安全或健康等目的可以进行的特定种类个人数据处理，该处理行为的数据控制人（处理人）可以豁免本法规的许多义务性规定。

（二）个人信息保护法的具体解释和执行规则进一步完善

依托个人信息保护基本立法，结合行业应用实践出台更富有操作性的具体执行规则成为各国的普遍做法。2013年9月，新加坡个人数据保护委员会发布了《个人数据保护法关键概念咨询指南》和《个人数据保护法指定主题咨询指南》，进一步明确了“个人数据”的含义、法律的适用范围、企业获得同意的方式以及应当采取的技术安全措施。对于实践中最令企业困惑的相关问题，如IP地址是否属于个人信息、

Cookie 信息是否应当适用个人信息保护法等作出了明晰的回答，为企业提供了更为明确的行为指南。2012 年 11 月 29 日，澳大利亚通过了对 1988 年《隐私法》的修正案，也进一步明晰了隐私保护的原则和具体方针。2013 年 6 月，欧委会制定了有关数据泄露通知制度的具体执行规则，明确了电信运营商以及互联网服务提供商在其用户个人数据丢失、被盗以及以其他方式泄露后，应当采取哪些措施才被认为充分履行了数据泄露通知义务。

★ 专栏：新加坡《个人数据保护法》咨询指南

2013 年 9 月，新加坡个人数据保护委员会颁布了《个人数据保护法》咨询指南，包括《个人数据保护法关键概念咨询指南》和《个人数据保护法指定主题咨询指南》。

1.《个人数据保护法关键概念咨询指南》

在《个人数据保护法》中，个人数据被界定为：能识别出个人的数据，或者通过该数据和其他相关的信息可以识别出个人。咨询指南中指出，个人数据概念是较为宽泛的，不管是正确的或者错误的，也不管是电子形式还是其他形式。个人数据包含可以直接识别出个人的数据，如姓名，以及间接识别出个人的数据，如住宅地址，如果能够与个人相关联识别出个人，就是个人数据。

立法不适用的个人数据：

- 企业联系信息；
- 已经保存超过 100 年的个人数据；
- 已经死亡超过 10 年的死者的个人数据。

其中，企业联系信息是指个人姓名、职位、企业电话号码、企业地址、企业电子邮件地址、企业传真号码或者其他关于个人的类似数据。

关于同意。企业最好的获得同意的方式是通过书面方式或者通过某种途径记录，以便今后提供证明。口头同意的方式也可以，但是机构最好通过某种记录的方式，将口头同意的时间记录下来。

关于告知用户。机构应当建立适当的政策和程序来明确个人数据收集的目的。机构最好以书面形式告知个人，如通过服务协议、数据保护声明。企业不需要把所有的与收集、使用、披露个人数据目的相关的活动都告知用户，只要把直接与目的相关的活动告知即可。

保护义务。机构应当：

- 设计和建立安全防护，以适用个人数据的特征和可能遭遇的安全损害；
- 找到可靠的和训练有素的人来负责信息安全；
- 执行强有力的措施和程序，确保各种层次的个人数据的安全；
- 准备好应对信息安全漏洞。

机构最好能够进行安全风险评估。

保留限制义务。保留限制义务不限定机构保留数据的具体时间，而是由每个机构根据其自身收集个人数据的用途来决定。虽然立法没有限制具体的时限，但是机构应当遵循相关的法律或者行业组织要求。

不要呼叫登记。不要呼叫登记最初可能会涵盖语音呼叫、文本信息和传真。

指定的消息：商业性质的营销消息应当是个人数据保护法中规定的。

该机制适用于通过所有方式发送消息，如语音呼叫、SMS，以及其他使用新加坡电话号码的数据发送应用程序，如“Whatsapp”，“iMessage”或者“Viber”。

2.《个人数据保护法指定主题咨询指南》

(1) 关于匿名化。

什么是匿名。在处理过程中去除识别信息，剩余的信息不能识别到个人。

匿名化就是将个人数据转化成一种数据，这种数据无论是本身还是通过机构已经获得的或者可能获得的其他数据都不能识别到个人。

为什么要匿名化数据。匿名化数据之后就可以不适用于个人数据保护法中的相关规定。

匿名化的限制和挑战。原始数据本身的特点决定了在匿名化的过程中需要去除多少数据。有些数据本身信息量就非常丰富，如人像照片，这样的信息如果去除身份的识别性之后该数据就几乎没有什么用处了。另外，有些匿名化的方法可能匿名了部分个人数据，但是其他的个人数据仍然不能匿名化。

匿名化数据与数据完整性之间还存在矛盾。匿名化数据不能保存数据有用的部分，以及数据具有潜在用途的内容。

重新鉴定和风险。机构在向其他机构公布或者披露个人数据时，应当考虑重新鉴定的风险。

重新鉴定风险的评估和管理，可以通过以下手段降低再鉴定的风险：

- 使用强大的匿名化技术；
- 限制信息披露的范围；
- 对数据的使用和披露施加额外的强制性限制；
- 实施严格的程序，包括管理匿名数据使用的过程；

■ 当数据没有商业和法律上的用处时，制定严格的销毁数据的程序和措施。

委员会和司法机构在考虑数据是否会被视为个人数据时，会考虑其重新鉴定的风险，如果风险高，就视为个人数据。

（2）在线活动。

IP地址是不是个人数据？IP地址单独来看不是个人数据，但是如果和其他的个人在网络设施上留下的信息一起比对，可以识别个人。如果机构收集的与IP地址相关的信息越多，例如该IP地址购买的项目，以及该IP地址其他的网络活动，就可能识别到个人。

使用Cookies是否需要获得同意。

Cookies的使用目的决定了其存储的时间不同。《个人数据保护法》适用于使用Cookies收集、使用和披露个人数据的行为。

并不是所有的Cookies都收集个人数据。会话Cookies只收集用于网站视频的技术数据，这种情况就不需要获得同意。

对于用户已经明确要求的互联网活动，则不需要获得同意，因为用户已经知道收集、使用、披露的目的。例如，传输个人数据是服务于网络通信，存储个人在Web表单中的信息是服务于在线购买活动等。那些不通过Cookies收集、使用和披露个人信息就无法实现的活动，则用户被视为同意提供个人数据。

不要呼叫登记规则。2013年10月，个人数据保护委员会发布了“不要呼叫登记的具体规则”。有三类DNC注册：拒绝语音呼叫注册、拒绝文本信息注册、拒绝传真信息注册。

从2014年1月2日开始，希望向新加坡用户进行电子推销的机构需要提交他们的电话号码名单，以检查是否在登记数据库中。要使用不要呼叫登记的具体服务、机构和个人应当在DNC网站上申请一个账户，每个机构/个人只能申请一个主账户。申请账户需要交纳一次性的费用。一共有三种类型的账户：在新加坡注册的机构、未在新加坡注册的境外组织和个人。

（三）儿童等特殊敏感信息受到更为严格的法律保护

2013年7月1日，美国联邦贸易委员会FTC修订后的《儿童在线隐私保护法案》（COPPA）规则正式施行。此次规则修订的目标是确保父母能够全方位参与到儿童的在线活动过程中，并且能够对任何人

收集儿童信息的行为有所知晓，同时，保护网络创新，保障互联网上能够提供越来越多的在线内容供儿童使用。规则要求在儿童父母未知、未获得其同意的情况下，对于那些专门针对儿童的 Apps 和网址，不允许第三方通过加入插件（plug-ins）来获得儿童信息。2013 年 9 月 23 日，美国加州通过《商业和专业条例》，明确 18 岁以下未成年人有权要求网络服务提供商删除个人信息。澳大利亚修订后的《隐私权法》也明确了对于敏感信息的收集和处理必须获得数据主体的明确同意，并对个人健康医疗信息以及基因信息的收集和使用制定了更为具体的规范。2012 年 7 月 25 日，英国司法部发布了《2012 数据保护（敏感个人数据）法令》（以下简称“2012 法令”），2012 法令明确了按照《1998 数据保护法》处理敏感个人数据的情况。

（四）数据泄露通知制度被更广泛引入个人信息保护立法

数据泄露通知制度是指在用户个人数据丢失、被盗以及以其他方式泄露后，数据控制者应当及时通知主管机构及当事用户。该制度为美国隐私保护立法首创，但近两年来被各国广泛采纳。欧盟 2011 年修订通过的《电子通信行业隐私保护指令》引入了该项制度，2013 年欧委会制定了数据泄露通知制度的具体执行规则，并将其上升为条例层级，这意味着该制度将直接在欧盟 28 个成员国得到适用。欧盟的数据泄露通知制度与美国相比更为严格，它要求：在发现泄露事件的 24 小时内，应当通知主管机构。如果在 24 小时之内不可能完成披露，则应当在 24 小时内提供一份初始的信息，其后在 3 天内补充其他信息。2013 年 5 月 29 日，澳大利亚司法部向国会提交了隐私法（隐私警告）的修正草案。作为对 2012 年隐私法修正案的再次修正，此草案对强制通知制度（Mandatory Notification）进行了要求，要求信息管理者在发生严重的数据泄露时，必须及时通知澳大利亚信息委员会以及受影响用户。

五、积极探索反垄断法适用互联网新规则

（一）美国《横向合并指南》（2010年版）大大降低了相关市场界定的重要性

2010年8月19日，美国司法部（DOJ）和联邦贸易委员会（FTC）正式联合发布了《横向合并指南》（Horizontal Merger Guidelines）（2010年版，以下简称“新指南”），替换1992年两部委共同颁布、1997年进行部分修订的《横向合并指南》，该指南对于美国的合并控制实践有着重要的指导意义。新指南在内容上进行了很大的调整与扩展^①，其修订的突出特点之一是合并审查的制度框架更为灵活，打破了旧指南确定的“五步分析法”，对市场界定进行了因应实际的改革，新指南不要求对每起水平合并案件都进行相关市场界定，大大降低了相关市场界定这一合并审查传统反垄断法适用起点的重要性。新指南强调，有关竞争效果的证据也能够支撑对相关市场的界定。比如，如果能够证明因提供一组产品的重要竞争者的减少而导致这一组产品价格的大幅上升，这本身就能够说明这组产品构成了一个相关市场。

★ 专栏：美国《横向合并指南》（2010年版）

新指南将市场界定的主要功能明确为两项：首先，市场界定有利于具体确认产生竞争关注的商业及地域边界；其次，市场界定可以让执法部门确定市场参与者并测量市场份额与市场集中度。

新指南指出，执法部门的分析不需要从市场界定开始，市场界定只是执法部门在评估竞争效果时可能运用的一系列工具中的一种，当能够获取反映竞争效果的直接证据时，执法部门将更倚重那些直接证据而非市场界定。新指南强调，有关竞争效果的证据也能够支撑对相关市场的界定。比如，如果

^① 内容涉及概论、反竞争效果证据、目标消费者与价格歧视、市场界定、市场参与者与市场份额及市场集中度、单边效应、协同效应、强势买方、市场进入、效率、破产、竞争性买方合并以及部分收购 13 个部分。

能够证明因提供一组产品的重要竞争者的减少而导致这一组产品价格的大幅上升，这本身就能够说明这组产品构成了一个相关市场。

就市场参与者的判定，新指南提到，那些当前不在相关市场上，但面临一项SSNIP时却可能快速进入市场供应产品并且不产生明显的沉没成本（Sunk Costs）的企业，也可被视为市场参与者。新指南指出，在大多数情况下，执法部门都基于相关市场中实际或预期的收入来测量企业的市场份额。

（二）欧盟采取相关市场界定与市场结构分析两种路径判定互联网滥用市场支配地位的行为

欧盟一方面采取相关市场界定方法应用于判定互联网市场支配地位，另一方面也直接采取市场结构分析的路径判定构成市场支配地位及其滥用的行为。欧盟认为，可从以下方面判断企业具有市场支配地位：如果一家企业在很大程度上无须顾忌其竞争对手、采购方或供给方的反应，我行我素地开展经营，则它就具有市场支配地位；或者没有其他竞争者或没有受到实质性竞争；又或者相对于其他竞争者具有突出的市场地位——市场份额、财力、采购/销售渠道，与其他企业的关联关系，其他企业进入市场的法律或实施障碍。另外，可从以下方面通过认定企业纵向一体化能力来直接判定其具有支配地位：提供富有差异性的产品或灵活调整供需产品的能力，上下游交易相对人对被考察企业的依赖性，企业经济实力，技术条件和创新能力等^①。

★ 专栏：欧盟《欧盟运行条约》第101和第102条

自《马斯特里赫特条约》建立欧洲联盟以来，历经《阿姆斯特丹条约》、《尼斯条约》的变革，在挑战接受《欧洲宪法条约》失败之后，27个会员国于2007年12月31日在里斯本采取折中方案签署了《修正欧洲联盟条约与欧洲共同体条约之里斯本条约》（简称《里斯本条约》）。该条约包含两部分重

^① 刘旭. 奇虎诉腾讯滥用市场支配地位案中的市场支配地位认定[J]. 电子知识产权, 2013(4)。

主要内容，即分别修订了《欧洲联盟条约》和《欧洲共同体条约》（以下简称《欧共体条约》），前者保持原名，后者则更名为《欧盟运行条约》。对于具体的竞争规则也相应地从原来《欧共体条约》第81条和第82条规定，变为《欧盟运行条约》第101条和第102条，这两条也是《欧共体条约》欧盟竞争法的核心条款。

《欧盟运行条约》第101条（1）规定如下：所有可能影响成员国间的贸易，并以阻碍、限制或扭曲共同市场内的竞争为目的或有此效果的企业间协议、企业协会的决议和一致行动，均被视为与共同体市场不相容而被禁止，尤其是下列行为：（a）直接或间接地固定购买、销售价格，或其他交易条件；（b）对生产、销售、技术开发和投资进行限制或控制；（c）划分市场或供应来源；（d）对同等交易的其他贸易伙伴适用不同的条件，从而使其处于不利的竞争地位；（e）使合同的缔结取决于贸易伙伴对额外义务的接受，而无论是依其性质或按照商业惯例，该额外义务均与合同的标的无关。

★ 专栏：欧洲《关于为欧洲共同体竞争法界定相关市场的委员会通知》

基于《欧共体条约》第85条和第86条的条例，特别是关于第17号条例的表格A/B的第六部分，以及有关对共同体规模的集中控制的第4064/89号条例的表格CO的第六部分已经规定了以下定义。

相关产品市场定义如下：

“一个相关产品市场是指根据产品的特性、价格及其用途，被消费者认为它们是可以相互交换或者相互替代的所有产品和/或服务。”

相关地域市场定义如下：

“相关地域市场是指这样一个地域，即相关企业在这里参与供应和购买产品或者服务，且它们在这个地域内的竞争条件基本是一致的，由于与相邻地域市场的竞争条件明显不同，从而可将其与相邻区域区别开来。”

★ 专栏：德国《反限制竞争法》^①

2005年6月，德国议会通过了《反限制竞争法》第7次修订法案。同年7

① 方小敏、李淳、杨娟译，《德国〈反限制竞争法〉（2005年第7次修订）》，《中德法学论坛》第4辑。

月12日,联邦政府公布了《反限制竞争法》第7次修正案,规定本次修订追溯至2005年7月1日开始生效。

第一条 禁止限制竞争协议

禁止以阻碍、限制或扭曲竞争为目的或者产生阻碍、限制或扭曲竞争后果的企业间协议、企业联合组织的决议以及协同行为。

第十九条 滥用市场支配地位

(1) 禁止一个或多个企业滥用市场支配地位。

(2) 如果一个企业作为某类商品或者工商业服务的供应者或需求者,在相关产品市场和地域市场上符合以下条件,即具有市场支配地位:

① 没有其他竞争者或者没有面临实质上的竞争。

② 相对于其他竞争者具有突出的市场地位。在此,特别要考虑该企业的市场份额、财力、进入采购或者销售市场的渠道,与其他企业的联合,其他企业进入市场所面临的法律上或事实上的障碍,本法适用范围内和适用范围外的企业与该企业之间存在的现实的或潜在的竞争,该企业将其供应或者需求转向其他商品或者服务的能力,以及市场相对方转向其他企业获得商品或服务的可能性。

两个或者多个企业作为某类商品或者工商业服务的供应者或需求者,相互之间不存在实质上的竞争,并且它们作为整体满足第1句规定的条件,则该两个或多个企业具有市场支配地位。

本法所规定的相关地域市场的范围,可以广于本法的适用范围。

(3) 一个企业至少占有1/3的市场份额,推定它具有市场支配地位。由多个企业组成的整体具备以下条件时,推定其具有市场支配地位:

① 3个或3个以下企业组成的整体,共同占有50%的市场份额。

② 5个或5个以下企业组成的整体,共同占有2/3的市场份额,但企业能够证明,它们之间存在实质性竞争,或者企业组成的整体相对于其他竞争者并不具有突出的市场地位的,不在此限。

(4) 滥用尤其存在于下列情况中,即如果一个占市场支配地位的企业作为某类商品或者工商业服务的供应者或者需求者:

① 无实质性正当理由严重损害其他企业参与市场竞争的可能性。

② 提出与有效竞争环境下理应获取的报酬或其他交易条件相背离的报酬或交易条件;在此,特别应当考虑在有效竞争的同类市场上企业可能采取的行为方式。

③ 提出的报酬或其他交易条件与它自己在其他同类市场上向同类购买人要求的报酬或其他交易条件比较相差甚远,且无实质性正当理由。

④拒绝其他企业以合理对价进入其拥有的网络或其他基础设施，导致另一个企业由于事实上或者法律上的原因无法在前置或者后置市场上作为占市场支配地位的企业的竞争者从事经营活动；但是，占市场支配地位的企业能够证明因为运营条件或者其他原因导致网络或其他基础设施的共同使用不可能或者不可期待的除外。

（三）互操作性、标准化和专利是当前互联网竞争行为的重要特征

在一体化日益加强的互联网经济中，互操作性可以让不同开发者开发的不同平台和应用互相兼容，从而提高对用户的价值。然而，互操作性也导致了竞争和互补性的产品的发展，可能会使得开发者抵触互操作性，尤其是那些占据支配地位的产品的开发者。而自愿公开应用程序的接口是企业实现互操作性的普遍做法，自愿公开可以促进创新，但是也会对公开方和接受方企业带来风险。一个争议的问题是竞争法在何种程度上可以强制占支配地位的企业公开其不愿意公开的互操作性信息。技术标准是互联网经济中促进互操作性的一种手段。如果一项标准经过良好的设计、是真正需要的而且被广泛采纳，它也能促进创新。然而，标准化并不能解决所有的互操作性问题。根据公平、合理和非歧视性原则进行专利授权，能够降低专利权人可能通过专利挟持技术标准的风险，近年来互联网技术的专利问题和专利拥有者独占专利问题导致了越来越多的诉讼。欧盟按照公平、合理和非歧视的原则确保互操作性和标准准入，即“FRAND”承诺。在 ICom and Rambus 的案例中，欧盟根据竞争规则予以介入。在复杂的互联网反垄断案例中，欧盟委员会支持开放市场和互操作性的方法，这种方法能促进创新和降低成本^①。

① OECD, The Digital Economy 2012, DAF/COMP(2012)22, 07-Feb-2013.

（四）韩国积极探索竞争执法机构和行业监管机构之间的协调配合机制

竞争执法机构的目标是鼓励竞争，行业监管机构某些情况下为实现产业政策目标可能会采取反竞争措施，二者必然存在一定矛盾和冲突。而且行业监管机构在其管辖范围内执行竞争法，一定程度上存在排除一般性的竞争法在特定行业适用的倾向。韩国解决竞争执法机构和行业监管机构之间的职责交叉主要采取三种方式：一是立法的事前协商（Statutory Prior Consultation），二是改进反竞争条例（Improvement of Anticompetitive Regulation），三是严格打击由行政指导引起的卡特尔（Strict Enforcement Against Cartel Caused by Administrative Guidance）^①。

^① Dongwon Suh, To Be a Better Competition Agency: KFTC 30-year-history & Suggestions on the future direction, 6th Seoul International Competition Forum, Sep. 15, 2010.

第三章 国际互联网管理体制

互联网管理体制是指一国对互联网管理机构设置、职能任务划分及其相互关系等方面的制度规定，是互联网管理的组织基础。各国在政治体制、经济发展、信息化发展水平等方面的差异，决定了互联网管理体制各具特色。但是，互联网作为一种普遍的信息化应用，也使得各国互联网管理体制体现出诸多共性。

一、多数国家未设立专门、统一的互联网管理机构

互联网已深入渗透到社会生活的方方面面，因此，绝大多数国家并没有设立专门、统一的互联网管理机构，而是由多个政府部门依据法律授权，对涉及本部门职责的互联网事务进行管理。

一类是传统政府部门，这些部门大多处理与自己的传统职能有着密切联系的互联网事务。例如，各国电信监管机构大多扮演互联网行业发展推动者的角色，承担促进互联网基础设施建设，鼓励互联网业务创新和市场竞争，保障互联网网络与信息安全等职责。例如，无论是美国 FCC，英国 OFCOM，还是日本总务省，这些电信监管机构不仅广泛参与互联网管理事务，还深度参与互联网行业政策的制定。从目前来看，电信监管部门涉及的互联网管理事务包括：互联网基础设施发展与规划、互联网资源政策制定、互联网接入市场竞争规范、互联网业务管理、网络与信息安全管理等。这一方面与互联网本身是从电信网络平台发展而来有关，电信监管部门对于互联网的管理有着天然的历史继承性；另一方面，作为基础设施和平台管理者的角色，电信监管部门也不可避免地参与互联网诸多事务的管理，与其他许多政府

部门存在着协助、配合关系。警察、安全机构主要负责打击网络犯罪活动，商务经济部门对电子商务进行管理，文化部门对网络版权进行管理。

另一类互联网管理机构是为应对互联网带来的新的管理问题，而专门成立的组织机构。这一类机构有的下设在传统政府部门之下，对传统政府部门负责，如大部分国家在电信监管机构之下设立的互联网信息中心，承担着互联网发展数据统计、产业调查、IP 地址、域名资源分配管理等职责；有的则是专门新设立的独立监管机构，例如，为应对数据保护和垃圾邮件问题，英国出台了《个人数据保护法》，并依据该法成立了独立的监管机构——信息委员办公室，由该机构履行公民个人数据保护等管理职责。

二、各国互联网管理机构的设置、职责一般以法律形式予以明确

绝大部分行政部门依据法律授权，实施对互联网的各项管理活动，特别是专门成立的部门，其设立、组织机构、职能都是以法律形式予以明确。例如，美国电信监管机构 FCC 主要依据《通信法》实施管理活动，日本总务省依据《网络服务商责任法》、《禁止非法链接行为法》、《反垃圾邮件法》、《个人信息保护法》等法律履行互联网管理职责，韩国互联网振兴院依据《互联网资源法》对域名、IP 地址等资源实施管理活动。

三、设立互联网政策议事咨询机构，提供政策发展建议

除管理机构之外，很多国家还设立互联网政策议事咨询机构，对互联网管理引发的新问题提供政策建议。这些咨询机构大多采取“委员会”的组织方式，广泛吸收各相关政府部门、行业代表、社会人士参与互联网建设与管理，增强互联网决策过程的民主性和科学性，此外，

对于互联网新生事物和问题，“委员会”机构提出的政策建议也更易被公众所接受。例如，韩国在个人信息保护方面，专门设立了审议委员会，对相关政策和制度改善进行政策咨询；新加坡也成立了电子商业政策委员会对相关政策制定开展咨询。

四、设立公共事业性机构，协助政府促进业务开展

很多国家在政府部门之下设立公共事业性机构，协助政府开展业务促进方面的工作。这些机构大多接受政府部门的领导和预算监督，承担培育、促进重要业务发展的职责。例如，韩国文化体育观光部专门下设了韩国游戏产业振兴院，具体负责网络游戏产业发展的有关事务，协助韩国游戏公司在全球市场推广韩国游戏产品，培育网络游戏文化，扩展游戏产业发展基础，培养游戏产业人才。韩国知识经济部下设的韩国电子商务振兴院也具有类似的功能。在其他国家，例如美国、英国也有各种非营利机构和自律组织参与促进相关互联网业务发展。

五、互联网网络安全机构所属类型多样

互联网的关键基础设施属性已被各国广泛认可，网络安全不仅事关国家经济社会的正常运转，也直接关系到国家安全。因此，各国不仅在政府机构，如电信监管机构、警察部门、安全部门设立专门的网络安全管理机构，在军队中也开始成立专门组织应对网络安全问题。例如，韩国在政府机构中设立互联网与安全局，负责保障国家互联网基础设施安全，免于黑客攻击、垃圾邮件泛滥和其他恶意侵犯等。同时，韩国也在军方成立了“网络安全司令部”。英国参与网络安全管理的机构也呈现多样化特点，如通信监管机构 OFCOM、政府部门英国商业创新和技能部。此外，英国还专门成立了英国电子通信抗毁性及应对小组，国家基础设施安全协调中心。同样，美国在网络安全方面也有相当数量的机构承担网络安全管理职责。

六、互联网内容管理机构行业化、民间化趋势逐步显现

在互联网内容管理方面,各国在机构设置上有着行业化、民间化的趋势。为解决互联网上的违法与不良信息泛滥问题,多数国家设立了信息内容举报中心,并作为一个公共事业机构运营。政府不直接干预具体管理事务,更多的是在公众教育、宣传服务方面发挥作用。例如,英国的互联网观察基金会 IWF,德国自律内容标准制定机构 FSM,等等。这些内容管理机构一般采取的管理措施有:①接受网民举报与咨询,依据相关法律法规对违法和不良信息进行审议和判定。②判定对青年人有害的网站,如服务器不在本国境内,则更新本国禁止接入的网站数据库,向 ISP 提供最新数据库,建议 ISP 进行封堵;如果服务器在境内,则向存储该内容的服务商发出内容删除通知,服务商应当及时删除相关内容,并为后续的司法调查保存记录。③提供互联网分级服务,支持互联网内容提供商对自己的内容进行自觉标注,并通过提供过滤软件和相关技术保护互联网用户远离不良信息侵扰。

第二篇

国内篇



第四章 我国互联网立法概述

20 世纪 90 年代以来,我国互联网法律制度经历了一个从无到有的建设过程。尤其是 2000 年以后,随着互联网逐步进入商用领域和实行市场化运作,我国有关互联网的立法活动也呈上升趋势,先后颁布了《全国人民代表大会常务委员会关于维护互联网安全的决定》、《互联网信息服务管理办法》等一系列法律法规。

目前,我国专门关于互联网的法律法规中,共有法律 3 部(其中两部为全国人民代表大会常务委员会颁布的法律性文件),行政法规 6 部,部门规章约 30 余部,司法解释 5 部。

从立法内容看,我国的互联网法律主要可分为基础网络管理、资源管理、业务管理及安全管理四个方面。

一、我国互联网基础网络管理立法

我国互联网基础网络管理类立法的主要内容集中于互联网基础设施的建设、网络连接、双边互联互通及基础网络设施的管理。工业和信息化部是互联网基础网络的管理部门,2000 年原信息产业部出台的《电信条例》(国务院令第 291 号)建立了基础网络管理的基本法律框架,2001 年出台的《互联网骨干网间互联服务暂行规定》和《互联网骨干网间互联管理暂行规定》两个部门规章,对互联网骨干网间互联、国家级交换中心、成员网络及其管理规则作了明确规定。此外,1996 年的《计算机信息网络国际联网暂行规定》(国务院令第 195 号)也涉及了基础网络管理的立法内容。

二、我国互联网资源管理立法

互联网域名和 IP 地址是互联网管理的基础。通过域名或 IP 地址，可以实现对行业发展的动态掌握和对信息源的追溯，从而在加强行业统计分析、追查网络违法行为责任人等方面起到重要作用。作为行业主管部门，工业和信息化部（原信息产业部）陆续发布了《中国互联网络域名管理办法》（信息产业部令第 30 号）和《互联网 IP 地址备案管理办法》（信息产业部令第 34 号），规定域名注册服务遵循“先申请先注册”原则，对在我国境内设置并运行域名根服务器的域名根服务器运行机构、域名注册管理机构和域名注册服务机构实行许可管理制度，并建立了对基础电信业务经营者、公益性互联网络单位和中国互联网络信息中心的 IP 地址备案制度。此外，2001 年最高人民法院公布的《关于审理涉及计算机网络域名民事纠纷案件适用法律若干问题的解释》（法释〔2001〕24 号），也对涉及计算机网络域名注册、使用等行为的民事纠纷案件的管辖、行为认定等作出了具体规定。

三、我国互联网业务管理立法

我国对互联网业务的规范和管理，主要体现在《电信条例》（国务院令第 291 号）、《互联网信息服务管理办法》（国务院令第 292 号）、《电信业务经营许可管理办法》（工业和信息化部令第 5 号）、《非经营性互联网信息服务备案管理办法》（信息产业部令第 33 号），以及其他部委关于互联网新闻信息服务、网络文化、网络支付等行政法规和规章中。

从内容分类上看，主要可以分为互联网通信类业务、互联网视听节目类业务、互联网新闻信息类业务、互联网电子商务类业务、互联网游戏及娱乐类业务和互联网金融、医疗、教育、印刷等业务。

互联网通信类业务的立法规定主要是原信息产业部于 2006 年出台的《互联网电子邮件服务管理办法》（信息产业部令第 38 号），对提

供电子邮件的条件、电子邮件服务器 IP 地址实行登记管理等问题作了详细规定；互联网视听节目类业务的立法有国家广电总局和原信息产业部于 2007 年出台的《互联网视听节目服务管理规定》（国家广电总局、信息产业部令第 56 号）和广电总局在不同时期所发布的一系列规范性文件所构成；互联网新闻信息类业务的立法有国务院新闻办公室和原信息产业部于 2005 年公布的《互联网新闻信息服务管理规定》，这个部门规章对互联网新闻信息服务和新闻类网站的建设等问题进行了规定，同时，也建立了互联网新闻信息服务单位申请设立和审批设立制度；互联网电子商务类业务的立法集中于电子签名、电子认证、发展电子商务等内容，主要有《电子签名法》（主席令第 18 号）、《电子认证服务管理办法》（工业和信息化部令第 1 号）和一系列规范性文件；互联网游戏及娱乐类业务的立法主要集中于网络游戏的内容、网络游戏经营单位自我约束机制等方面，主要是文化部于 2010 年出台的《网络游戏管理暂行办法》（文化部令第 49 号）和 2011 年出台的《互联网文化管理暂行规定》；互联网医疗保健类业务立法主要是原卫生部 2009 年出台的《互联网医疗保健信息服务管理办法》（卫生部令第 66 号）。

四、我国互联网安全管理立法

我国颁布、施行的有关信息安全管理方面的文件和法规众多，设定了我国信息安全一系列重要的规范和制度，厘清了我国信息安全领域的行政监督管理职能，比较充分地规范了我国信息安全领域的重大事项、法律关系和法律责任。工业和信息化部制定了《通信网络安全防护管理办法》（工业和信息化部令第 11 号），确立了互联网安全等级保护、安全评测和风险评估制度，明确了灾难备份、应急处置等制度，并通过对基础电信企业信息安全责任、互联网企业网络安全信息通报及木马和僵尸网络监测与处置机制等配套规定，建立起一套较为完善的网络安全防护和应急处置制度。

第五章 我国互联网立法热点

2013 年国内互联网领域立法进展总体平稳。从内容上来看，集中在几个方面：一是个人信息保护立法取得重大进展，二是电子商务领域立法进程加快，三是互联网信息服务市场秩序进入法制化轨道，四是网络版权保护力度进一步加强，五是网络信息安全立法逐步启动。

从监管趋势来看，互联网监管呈趋紧态势，一方面，对用户权益保护、网络版权保护、信息安全保护的力度逐渐加大；另一方面，监管范围逐步扩大，如电子商务、互联网信息服务市场秩序等领域都相继被纳入法制化轨道。

一、我国个人信息保护立法取得重大进展

2012 年年底，全国人民代表大会常务委员会通过了《全国人民代表大会常务委员会关于加强网络信息保护的决定》（以下简称《人大决定》），首次以法律的形式明确规定保护公民个人及法人信息安全，建立网络身份管理制度，明确相关各方的权利、义务和责任，赋予政府主管部门必要的监管手段，对进一步促进我国互联网健康、有序发展具有重要意义。

1. 《人大决定》

（1）保护的信息范围。《人大决定》将其保护的信息界定为“公民个人电子信息”，该信息包含了两类信息：一是能够识别公民个人身份的信息，二是涉及公民个人隐私的信息。因此，从其保护的信息的内容范围看，是较为宽泛的，但从信息的载体形式看，《人大决定》

又将其限制为电子信息。考虑到当前个人信息侵害主要的传播途径是通过电子通信网络，因此《人大决定》所确定的保护信息范围能够覆盖和解决当前的主要问题。

（2）区分不同的主体。《人大决定》规范了三类主体：网络服务提供者、企事业单位、国家机关。这三类主体都有可能涉及对个人信息的商业化使用，但由于前两种主体对于商业使用的应用更为普遍，因此《人大决定》对于前两者的法律规制更为全面。

（3）保护的基本原则。《人大决定》一方面明确提出了个人信息保护的基本原则，如收集信息的合法、正当、必要原则；另一方面对于国际上保护个人信息的基本原则，如知情同意、透明等原则以法律条文规定具体行为规范的方式进行了体现。《人大决定》基本上囊括了国际上通行的基本原则，但受制于决定的文件形式，也剔除了一些其他原则，如信息质量原则、个人参与原则。此外，对于关键性的知情同意原则，《人大决定》并没有明确是明示同意还是默示同意，可以理解为包含了这两种同意模式，为下位法制定预留了空间。

（4）《人大决定》明确规定了技术措施。无论是针对网络服务提供者，还是针对国家机关，《人大决定》都突出强调了技术措施在保护个人信息安全以及监督管理工作中的重要作用，要求相关主体采取技术措施和其他必要措施，确保信息安全。

（5）《人大决定》规定了个人信息保护的三种救济渠道，包括民事诉讼途径，行政检举控告机制以及刑事责任追究机制。

总体来看，《人大决定》的条文较为简单，但覆盖问题却十分广泛。其正式颁布，是以法律形式宣示国家对个人信息提供法律保护，标志着我国在个人信息保护立法领域的重大突破，有利于我国在此基础上继续推动个人信息保护专门立法工作及为参与相关国际规则制定提供制度准备。

2. 工业和信息化部《电信和互联网用户个人信息保护规定》

2013年7月，工业和信息化部出台了《电信和互联网用户个人信息保护规定》（工业和信息化部令第24号），并于2013年9月1日起施行。该规定进一步明确了电信业务经营者、互联网信息服务提供者收集、使用用户个人信息的规则和信息安全保障措施等，是落实《人大决定》规定的制度和措施、切实保护用户合法权益的具体体现。

（1）明确工业和信息化部对于电信和互联网领域个人信息保护的行政管理职责。依照《人大决定》的规定，有关主管部门应当在各自职权范围内依法履行职责，采取技术措施和其他必要措施，防范、制止和查处窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为。作为电信管理机构和互联网行业主管部门，工业和信息化部负有对电信和互联网领域的用户个人信息保护的管理职责。

（2）依据《人大决定》，进一步明确有关个人信息保护的具体法律要求，包括：明确服务提供者保障用户个人信息安全的责任。例如，在岗位责任、制度流程、权限管理、介质管理、网络安全防护、安全风险评估、日志记录等方面提出具体要求，以切实贯彻《人大决定》中关于网络服务提供者应当采取技术措施和其他必要措施，确保信息安全的有关要求；明确电信企业和互联网企业在开展委托业务时转移用户个人信息的有关要求，如审查合作方有关个人信息保护的能力，通过合同明确双方对用户的个人信息保护责任。

（3）依托现有的电信和互联网监管制度，加强个人信息保护管理。例如，在许可年检审查制度中增加有关个人信息保护的考核，强化企业的信息保护管理责任；依托现有的重点监管制度，将个人信息保护纳入企业的信用管理和公示，加强对企业收集和使用用户个人信息的监督约束。

《人大决定》和工业和信息化部《规定》的相继发布,标志着我国个人信息保护工作取得了重大进展。一方面,《人大决定》以最高立法层级的形式对个人信息保护的要求作了明确规定,为各项工作的开展提供了上位法依据;另一方面,工业和信息化部《规定》从落实的角度对个人信息保护相关工作进行了细化,明确了责任主体、法定义务、罚则等。随着《人大决定》和工业和信息化部《规定》的发布和实施,我国个人信息保护工作进入了“有法可依”和“全面实施”的新阶段。

二、电子商务领域立法进程加快

随着电子商务的快速发展,电子商务立法受到广泛关注。2013年,电子商务立法进程大幅加快,未来我国电子商务领域将逐步统一纳入法制化轨道。

(一) 2013年电子商务领域出台的相关立法

1. 《网络发票管理办法》

2013年1月,国家税务总局审议通过并公布了《网络发票管理办法》(税务总局令第40号),明确规定开具发票的单位和个人必须如实在线开具网络发票。国家税务总局称此举将有助于加强对电子商务的监管,有利于保护消费者的合法权益。

针对“办法出台是为了对电商征税做准备”的外界猜测,国家税务总局予以了否定。网络发票是规范发票使用和税收征管,以及防控发票类违法犯罪的手段,而非针对网络购物和电子商务征税。网络发票改变了开具发票的手段,使得纳税人可以通过互联网开具发票,实现了发票在线开具、查询、购销等功能。网络发票具有成本低、填开数据真实、便于发票真伪查询、有利于税收征管等优点,并为进一步发展到电子发票奠定了基础。

2. 《关于修改〈中华人民共和国消费者权益保护法〉的决定》

2013年10月，全国人民代表大会常务委员会通过了《关于修改〈中华人民共和国消费者权益保护法〉的决定》（以下简称《消法决定》）。这是《中华人民共和国消费者权益保护法》颁布以来的首次大修，主要包括四大方面，其中之一就是规范网络购物等新型消费方式。此次大修增加了规范网络购物的内容，从侧面体现了国家最高立法层面对电子商务的重视，其中以下几个亮点值得关注。

（1）赋予了消费者在网络购物中的“后悔权”。

《消法决定》明确规定，除特殊情况外，消费者通过网络等方式购买的产品可以“七日内无理由退货”，从而提高了电子商务过程中对消费者权益保护的力度。“后悔权”的规定无疑最大限度地保证了消费者网上购物的权益，虽然从表面上看增加了电子商务企业的负担和成本，但是规定了例外的五种情形，对电子商务企业进行了合理保护，从长远来看，有利于规范电子商务市场经营，形成健康、有序的发展环境，同时也为电子商务企业长期良性发展提供了有利条件。

（2）网络购物中保护消费者知情权。

《消法决定》新增了一项要求：采用网络（电视、电话、邮购等）方式提供商品或者服务的经营者应当向消费者提供经营地址、联系方式、商品或者服务的数量和质量、价款或者费用、履行期限和方式、安全注意事项和风险警示、售后服务、民事责任等信息。通过列举的方式明确规定了采用网络方式提供商品或者服务的经营者应当告知消费者的各项信息，极大限度地保护了消费者在网络购物中的知情权，强化了网络购物的诚信建设，促进了电子商务市场秩序良性发展。

（3）强化网络交易平台提供者的监管责任。

《消法决定》新增了一项要求，网络交易平台提供者需要核验销售者或者服务者的真实名称、地址和有效联系方式，消费者合法权益

受到损害向销售者或者服务者要求赔偿时，可以要求网络交易平台提供者提供上述信息，网络交易平台提供者不能提供的，消费者可以要求其赔偿。对于网络交易平台提供者明知或者应知销售者或者服务者利用其平台侵害消费者合法权益，未采取必要措施的，需要与该销售者或者服务者承担连带责任。

《消法决定》的要求提高了网络交易平台提供者的监管责任。事实上，消费者通过网络获取商品或服务时，存在信息不对称的劣势，网络交易平台提供者相对更有能力和机会去获取销售者或者服务者的真实信息，因此对其苛以严责是合情合理的。同时，网络交易平台严重不作为或存在主观故意情形时需承担连带赔偿责任，是对消费者权益更有力的保护。

（二）电子商务领域相关立法起草工作取得积极进展

1. 《网络零售第三方平台交易规则管理办法（征求意见稿）》

2013年9月，商务部正式就部门规章《网络零售第三方平台交易规则管理办法（征求意见稿）》向社会公开征求意见。征求意见稿中规范的重点是交易规则制定和修改的流程，以保障利益相关方在规则制定、修改过程中的充分参与权，促使规则形成过程的公开化、透明化、规范化，不过并没有直接干涉平台及相关方在规则内容制定、修改上的自主决策权。

这将是我国首部规范“网规”的部门规章。商务部表示，目前交易规则多为电子商务企业单方面制定，难免在执行中出现相关方对交易规则的质疑，严重的话会影响公共利益。因此，把这些“网规”上升为法规监管范畴，实现“网规”的规范化，成为我国规范、发展电子商务的一个重要课题。同时，我国电子商务企业在多年实践中已经摸索并建立了一套相对完整的网络市场自我治理措施和交易规则，这

些规则对维护和保障网络市场快速、稳定发展起到了积极作用，该部门规章将对其中一些交易规则进行确认和固化。

2. 《食品安全法（修订草案送审稿）》

2013年10月，《食品安全法（修订草案送审稿）》公开征求社会意见。送审稿规定了网络食品交易第三方平台的责任及其应负的连带责任：网络食品交易第三方平台提供者应当取得食品生产经营许可证；应当查验入网食品经营者的许可证或者对入网食品经营者实行实名登记，承担食品安全管理责任。网络食品交易第三方平台提供者未履行规定义务，使消费者的合法权益受到侵害的，应当承担连带责任，并先行赔付。

送审稿关于网络食品交易的规定，将进一步强化对网络食品交易的监管，网络食品交易第三方平台也应当取得食品经营许可，加强第三方平台的管理责任。送审稿获得通过后，对食品安全的监管将从线下延伸到线上，有利于形成更加完善的食品安全制度环境。

3. 《电子商务法》列入立法计划

2013年，我国的电子商务快速发展，对传统商业领域、流通领域、金融领域、物流等服务业领域都产生了很大影响，并逐渐改变着人们的工作和生活方式。与此同时，也带来一些问题：一是行业监管方面，“政出多门”使得电子商务企业无所适从；二是市场秩序方面，诚信体系缺失；三是网络支付方面，便利性和安全性的双重要求对网络支付形成考验；四是税收管理方面，尚未针对电子商务采取优惠措施。目前，《电子商务法》的具体内容还无从得知，但上述几个方面无疑是立法亟须解决的重点问题。

2013年10月31日，第十二届全国人民代表大会常务委员会公布了五年立法规划，其中《电子商务法》被列为第二类项目（“需要抓紧

工作、条件成熟时提请审议的法律草案”）。这是电子商务立法的一个里程碑，此后，随着《电子商务法》纳入人大立法规划，电子商务立法进入新阶段。

三、互联网市场竞争立法不断加强

2010 年爆发的“3Q 大战”案件暴露出我国互联网信息服务市场秩序监管方面的法制空白。2011 年 12 月，工业和信息化部公布了《规范互联网信息服务市场秩序若干规定》（工业和信息化部令第 20 号）。该规定明确了禁止实施的侵犯其他互联网信息服务提供者权益的相关行为，为规制网络不正当竞争提供了法律依据，从一定程度上填补了互联网信息服务市场秩序监管法律制度的空白，有利于改观互联网信息服务的法制环境。

2011 年 1 月 7 日，国家工商总局公布了三个适用于互联网市场竞争的部门规章：《工商行政管理机关禁止垄断协议行为的规定》（国家工商行政管理总局令第 53 号）、《工商行政管理机关禁止滥用市场支配地位行为的规定》（国家工商行政管理总局令第 54 号）、《工商行政管理机关制止滥用行政权力排除、限制竞争行为的规定》（国家工商行政管理总局令第 55 号）。

2013 年 7 月 10 日，结合全国工商行政管理机关近年来查办的网络违法案件，国家工商总局公布了九类典型网络商品交易违法行为，以提升消费者的网络消费辨别力，强化行政机关在网络商品交易监管工作中的公示警示作用。九类典型网络商品交易违法行为包括：销售侵犯注册商标专用权商品；违反企业登记管理相关规定，伪造或冒用公司名称；使用与知名商品近似的名称、包装、装潢，造成与他人的知名商品相混淆，误导消费；利用网页发布与真实情况不符的企业或商品信息，进行虚假宣传；恶意诋毁，损害竞争对手的商业信誉、商品声誉；销售假冒伪劣商品，损害其他经营者或消费者利益；未经许可，

从事法律法规规定须取得营业执照方可从事的经营活动；违反相关规定，擅自泄露或出卖消费者个人信息；利用格式合同作出对消费者不公平、不合理的规定，侵害消费者权益。其中，“恶意诋毁，损害竞争对手的商业信誉、商品声誉”的行为具体采用方式分为三大类：第一大类为主观拦截竞争对手产品的默认设置与安装；第二大类为诱导卸载；第三大类为影响使用。

工业和信息化部第 20 号令以及国家工商总局的三个规章对规范互联网市场竞争起到了很好的作用，但目前行业主管部门的法定授权、执法资源及执法手段有限，在行为识别、取证、细则、专家机制等多方面存在执法困境，后续相应的市场竞争监管制度、机制等尚需配套。互联网企业违规成本较低，违规事件屡禁不止，而且互联网领域出现了大量新型的不正当竞争行为。例如，流量劫持行为、客户端干扰行为、商业抄袭行为、网络搭便车、竞价排名、网页抄袭、域名恶意抢注或使用、软件恶意不兼容、对搜索结果不合理人工干预、未经许可商业性使用他人产品 / 服务等行为，仍有待立法予以规范。

四、网络版权保护力度进一步增强

随着网络信息的快速发展和移动智能终端的广泛普及，网络信息的新业务、新应用、新业态不断出现，全方位、多层次满足了人们的消费体验。但是，由于网络信息具有无限开放的特点，给版权保护带来了众多问题和挑战。网络版权保护工作是一个长期、渐进的过程，也是一项综合性系统工程，需要法律、行政等多种手段协调推进。2013 年网络版权保护相关工作即遵循了这一思路。

（一）通过修法加大法律惩处力度

自 2013 年 3 月 1 日起，国务院新修订的《计算机软件保护条例》（国务院令 第 632 号）、《著作权法实施条例》（国务院令 第 633 号）、《信

息网络传播权保护条例》(国务院令第634号)三个行政法规正式施行,我国保护网络版权的力度进一步加强。我国现行的《著作权法》第47条规定了侵犯著作权的行政法律责任,其中设定的行政处罚包括罚款,但未对罚款数额作规定。上述三部修订的行政法规对罚款数额作出了具体的规定,为打击侵犯网络版权的行为提供了明确的法律依据。

(二) 行政执法持续打击网络侵权盗版行为

2013年6月19日,国家版权局、国家互联网信息办公室、工业和信息化部、公安部联合下发《关于印发〈2013年打击网络侵权盗版专项治理“剑网行动”实施方案〉的通知》,部署了自2013年6月20日起为期4个月时间打击各种网络侵权盗版行为的专项行动。主要围绕网络文学、音乐、影视、游戏、动漫、软件等重点领域以及图书、音像制品、电子出版物、网络出版物等重点产品,加强对重点音/视频网站、网络销售平台的监管力度。

“剑网行动”自2005年起已经连续开展了9年,通过查处案件、关闭非法网站、处理违法人员的方式,对网络侵权盗版活动予以了持续的打击,取得了明显的成效。自2012年起,在国家版权局、公安部、工业和信息化部的基础上增加了国家互联网信息办公室,大大增加了工作力度。

五、网络信息安全立法逐步启动

随着移动互联网技术的快速发展和海量数据的应用,特别是“棱镜门”事件带来的巨大影响,社会对网络信息安全的关注达到了前所未有的程度。

(一) 《关于加强移动智能终端管理的通知》

2013年4月,工业和信息化部下发了《关于加强移动智能终端管

理的通知》，对移动智能终端安全能力和预置应用软件提出了管理要求，提出移动智能终端应当符合《移动智能终端安全能力技术要求》通信行业标准的一级安全能力要求，并要求生产企业不得在移动智能终端中预置相关应用软件。

2013年，移动智能终端快速发展，在给用户带来便利的同时，各种新的安全问题也日益凸显，如未经用户允许收集用户信息、智能终端预置软件恶意“吸费扣费”、厂商最终投放市场的智能终端与入网检测时的备案不一致等，严重影响用户个人信息安全、损害用户合法权益、扰乱电信市场的正常经营秩序。《关于加强移动智能终端管理的通知》依据全国人民代表大会常务委员会《关于加强网络信息保护的決定》、《电信条例》、《电信设备进网管理办法》等有关规定，对移动智能终端进网管理作了进一步明确：一方面明确了移动智能终端入网的安全要求和检测标准，另一方面明确了终端生产企业预装应用软件的范围和要求。该通知于2013年4月发布、11月1日正式施行，给生产企业半年的过渡期，而在此期间内，也为电信管理机构治理智能手机预装应用软件背后的利益链提供了有力的政策支持。

智能手机预装应用软件背后利益链主要存在以下问题。

首先，目前智能终端出厂时预装大量应用软件的现象普遍存在，消费者无法获知终端是否被预装，无论通过官方渠道购买，还是通过其他代理渠道购买，智能手机都会被预装应用软件。其次，被预装的应用软件类型多样，良莠不齐。经媒体报道，消费者被预装的应用软件中，有不少涉及“吸话费”、“吸流量”等诈骗行为，令消费者防不胜防，消费者对被预装哪类应用软件，没有选择权；最后，预装应用软件中，存在无法被消费者卸载的情况，原因是用户没有智能手机的最高操作权限，但是消费者一旦获取最高操作权限后，官方保修点却以用户私自更改手机操作系统为由，不予保修，用户无法享受“三包服务”的合法权益。

该通知出台前,此类问题屡见不鲜,只是消费者投诉无门,而相关监管机构处理此类问题时,也缺乏必要的法律支撑,导致消费者往往选择隐忍态度,才令背后的利益方愈加猖獗。通知出台后,首先,明确了生产企业不得在移动智能终端中预置具有五类性质的应用软件,并进一步要求研究支撑机构对应用软件的类型进行细分,使监管机构对预装应用软件的行为具有了更强的掌控能力;其次,监管部门在对智能终端预置应用软件的安全管理上,有了法律上的支撑,对生产领域的手机厂商、运营商,流通领域的代理商及维修商的责任有了明确的划分,将会大大降低监管部门执法的难度。

但是,由于应用软件数目繁多,种类庞杂,涉及管理问题多种多样,该通知仍不能完全涵盖移动智能终端进网管理的方方面面,存在一些监管盲点,如对预装应用软件究竟可否被删除没有规定、预装应用软件改型后备案缺乏相关管理办法、终端定制备案的执行情况没有建立相应的报送制度等。我们相信,未来的监管将更好地应对智能终端快速发展带来的挑战。

（二）《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》

2013年9月,最高人民法院、最高人民检察院公布了《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》,针对利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等刑事犯罪的法律适用问题作出了若干规定,为这些犯罪的定性提供了明确的指引。利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等刑事犯罪,是伴随着信息网络的飞速发展而出现的新情况、新问题,虽然刑法对采用传统手段实施的上述犯罪早已作出了规定,但对于利用信息网络实施的上述犯罪,尚缺乏有针对性的、明确的、具体的规定,因此,在司法实践中存在法律适用不够明确的问题。司法解释的出台,是为

了确保法律适用统一，依法惩治、有效防范利用信息网络实施的诽谤等犯罪。对利用信息网络实施的犯罪予以打击，将净化网络空间环境，提高我国网络信息安全水平。

第六章 2013 年主要宏观政策

当前,我国互联网网络规模 and 用户规模已跃居世界首位,网络能力显著提升,政策环境不断完善,管理体系逐步优化,技术创新更加活跃,应用服务蓬勃发展,已涌现出一批知名互联网企业,形成了具有一定国际影响力和竞争力的互联网产业。随着移动互联网、云计算、物联网以及下一代互联网的迅猛发展,互联网将加速向各行业、各领域渗透,产业发展、变革、融合的趋势将更加明显,这将为我国的信息化建设和经济社会发展提供强大动力。我国互联网和信息化的飞速发展都离不开宏观政策的良好指引和推动,2013 年的信息消费、宽带中国、信息安全和两化融合及上海自贸区等相关政策措施,将成为进一步推动我国互联网和信息化发展的新引擎。

一、大力发展信息消费

2013 年 8 月 14 日,国务院正式发布《关于促进信息消费扩大内需的若干意见》(国发〔2013〕32 号,以下简称《若干意见》),提出建立促进信息消费持续稳定增长的长效机制。

(一) 出台背景

2013 年 4 月 17 日,国务院常务会议提出,要积极扩大国内有效需求,完善消费政策,开发和培育信息消费等新的热点。李克强总理多次批示要促进信息消费,抓紧就扩大内需提出相关举措,措施要既有利于当前稳定增长,更有利于长远调结构、转方式。根据上述要求和指示精神,工业和信息化部、国家发改委分别开展了《若干意见》起草和

有关政策研究工作。

5月下旬至6月初，工业和信息化部苗圩部长及四位副部长分五组赴北京、天津、长三角、珠三角等地密集开展深入专题调研，广泛听取地方政府、重点企业、消费者的意见和建议。

7月12日，国务院常务会议对《若干意见》进行了审议。8月14日，经修改后国务院正式下发。

（二）政策概况

《若干意见》总体要求：以深化改革为动力，以科技创新为支撑，围绕挖掘消费潜力、增强供给能力、激发市场活力、改善消费环境，加强信息基础设施建设，加快信息产业优化升级，大力丰富信息消费内容，提高信息网络安全保障能力，建立促进信息消费持续稳定增长的长效机制，推动面向生产、生活和管理的信息消费快速健康增长，为经济平稳较快发展和民生改善发挥更大作用。

《若干意见》中确定了促进信息消费的五大任务、六大支持政策，主要表现为：

- ★ 提出了信息消费规模快速增长、信息基础设施显著改善、信息消费市场健康活跃的主要目标。
- ★ 通过完善宽带网络基础设施，统筹推进移动通信发展，全面推进三网融合，加快信息基础设施演进升级。
- ★ 通过鼓励智能终端产品创新发展，增强电子基础产业创新能力，提升软件业支撑服务水平，增强信息产品供给能力。
- ★ 通过拓展新兴信息服务业态，丰富信息消费内容，拓宽电子商务发展空间，培育信息消费需求。
- ★ 通过促进公共信息资源共享和开发利用，提升民生领域信息服

务水平，加快智慧城市建设，提升公共服务信息化水平。

- ★ 通过构建安全可信的信息消费环境基础，提升信息安全保障能力，加强个人信息保护，规范信息消费市场秩序，加强信息消费环境建设。
- ★ 通过深化行政审批制度改革，加大财税政策支持力度，切实改善企业融资环境，改进和完善电信服务，加强法律法规和标准体系建设，开展信息消费统计监测和试点示范，完善支持政策。

（三）影响分析

“信息消费”作为国家经济发展战略，除了直接拉动消费、扩大内需之外，还有助于推进第三产业，特别是信息服务业的转型升级，并有望成为推动我国经济持续增长的新着力点。

通过《若干意见》的指导作用，政府部门推出扶持政策，引入民营资本竞争，将进一步完善信息服务业企业的结构，形成多层次、多领域的全面发展，让更多中、小、微型企业等加入进来，加快行业的创新，促进高层次信息服务水平的提升。同时，因为信息服务业对各行业的渗透作用，信息服务业的发展不仅能够带动行业本身的发展，也必将推动和引领相关行业的发展。

二、发展宽带成为国家战略

2012 年 8 月 17 日，酝酿已久的国家宽带战略正式发布：国务院印发《“宽带中国”战略及实施方案》（以下简称《战略方案》），旨在加强战略引导和系统部署，推动我国宽带基础设施快速健康发展^①。

^① 国家发改委答问《“宽带中国”战略及实施方案》，www.gov.cn，2013 年 8 月 19 日访问。

（一）出台背景

《战略方案》是在认真研究和充分考虑国际、国内发展形势基础上研究制定的。从国际看，宽带在抢占新一轮科技和产业变革制高点、塑造新时期国家发展新优势方面的战略先导作用日趋突出，已成为各国战略性基础设施的重要组成部分。据有关方面统计，自金融危机以来，发达国家和127个发展中国家发布并实施了宽带战略或相关行动计划，以加强统筹规划和战略指引，力图通过统筹政府和市场力量实现宽带超常规发展，以抢占国际竞争制高点。这些国家主要从3个方面进行了战略部署：一是加强系统规划，全面提升宽带发展水平。以光纤接入和新一代移动通信为重点加快建设高速宽带网络，以实现以农村宽带覆盖为重点缩小数字鸿沟，以支撑经济发展转型和改善民生服务为重点普及深化业务应用。二是加快网络空间战略布局，强化信息化条件下的国家竞争优势。以宽带为基础，着力提升网络空间发展能力，推进网络空间安全国际合作和网络空间国际规则的制定。三是加大政策扶持，优化发展环境。在财政补贴、税收减免、信贷优惠等系列政策措施方面加大支持力度；将电信普遍服务机制向宽带扩展；提供频谱、站址、管道等保障，加快推动无线移动通信发展。

从我国的情况看，当前正处于加快转变经济发展方式和全面建成小康社会的关键时期，宽带在经济、社会、科技发展中正发挥着越来越重要的作用。建设一个宽带、融合、安全、泛在的信息网络已成为我国未来发展的迫切需要和战略选择。一是转变经济社会发展方式要求深化宽带在经济社会各领域的应用。加快战略性新兴产业发展，要求强化宽带网络与新一代信息技术、生物医药、新能源、新材料、绿色智能建筑等产业的深度结合，推进产业融合创新。促进传统产业转型升级，要求深化宽带在研发设计、生产制造、经营管理等环节的集成应用，变革生产方式，推动制造业向柔性制造、绿色制造和服务型制造转变。发展现代服务业，要求深化宽带在商贸流通、金融交易、

生产服务中的基础平台作用，培育壮大电子商务、网络金融、现代物流等新业态，推进服务业规模化和网络化发展。二是推动创新型国家建设要求全面提升宽带能力。抓住当前新一轮技术变革机遇，激发国家创新活力，要求充分发挥宽带在科技创新中的协同平台作用，聚集和整合全球科技资源，加快对全球科技成果的学习利用，加速科学技术扩散和共享，促进全社会科技资源优化配置。三是创新社会管理和服务模式要求加快网络覆盖和普及。促进基本公共服务均等化，要求基于宽带网络提供远程教育培训、医疗卫生、社会保障等公共服务，延伸优质资源服务范围，创新服务模式。宣传主流声音，弘扬先进文化，要求通过宽带网络汇聚民意民智。创造新型就业机会、扩大就业规模、优化就业结构，要求加大宽带业务普及和应用创新。四是构筑网络空间竞争优势要求打造安全可控的宽带网络。当前网络空间竞争形势日趋复杂，网络信息安全挑战日趋严峻，要求加快建设和完善网络信息安全保障机制和管理支撑能力，实现网络空间的可靠、可信、可管、可控。

2013 年 7 月 12 日，国务院常务会议对促进信息消费进行了研究部署，其中明确要求加快“宽带中国”建设，挖掘信息消费潜力，促进信息消费持续稳定增长。当前我国研究提出“宽带中国”战略，目的就在于明确宽带的发展定位，通过加强顶层设计，统筹网络部署、技术研发、产业发展、应用服务和安全保障能力建设，加快完善相关政策和发展环境，有效支撑我国经济、科技和社会发展。

（二）政策概况

1. 发展目标

《战略方案》对总体目标和分阶段的实施目标都作了系统设计。在总体目标上，根据我国宽带发展的实际情况，针对目前存在的主要问题，《战略方案》围绕宽带覆盖、能力提升、宽带应用、产业

发展四个方面，提出了我国宽带发展 2015 年阶段性目标和 2020 年长期目标。

预计到 2015 年，通过战略实施，我国要初步建成适应国民经济和社会发展需要的宽带、融合、安全、泛在的下一代国家信息基础设施；固定宽带家庭普及率达到 50%，3G/LTE 用户普及率达到 32.5%，行政村通宽带比例达到 95%，学校、图书馆、医院等公益机构基本实现宽带接入。尤其是在城市和农村家庭宽带接入能力方面，《战略方案》提出，要在 2015 年基本达到 20Mbps 和 4Mbps 的水平，部分发达城市要达到 100Mbps。同时，在网络覆盖能力提高的同时，要实现宽带应用水平大幅提升，网络与信息安全保障能力明显增强。

预计到 2020 年，我国宽带网络基础设施发展水平与发达国家之间的差距大幅缩小，国民充分享受宽带带来的经济增长、服务便利和发展机遇。固定宽带家庭普及率达到 70%，3G/LTE 用户普及率达到 85%，行政村通宽带比例超过 98%。在城市和农村家庭宽带接入能力方面，战略提出要分别达到 50Mbps 和 12Mbps，发达城市部分家庭用户甚至可达到 1Gbps。同时，在技术创新和产业竞争力方面，将达到国际先进水平，并形成较为健全的网络与信息安全保障体系。

围绕上述发展目标，在《战略方案》中还分别提出了清晰的技术路线和发展时间表，形成了实施方案。在全面提速阶段（至 2013 年年底），我国将加强光纤网络和 3G 网络建设，提高宽带网络接入速率，改善和提升用户上网体验。在推广普及阶段（2014—2015 年），我国将在继续推进宽带网络提速的同时，加快扩大宽带网络覆盖范围和规模，深化应用普及。在优化升级阶段（2016—2020 年），我国将推进宽带网络优化和技术演进升级，宽带网络服务质量、应用水平和宽带产业支撑能力将达到世界先进水平。

2. 重点任务

针对当前我国宽带发展区域差距拉大、网络速率整体偏低,以及产业支撑能力有待提升等突出问题,《战略方案》从区域发展、网络升级、应用水平、产业能力和安全保障五个重点环节,分别提出了一系列重点任务:一是推进区域宽带网络协调发展。东部地区以提速和性能改善为主,中西部地区以推进宽带网络覆盖和普及为主,农村地区则强调因地制宜,采用有线、无线等多种接入手段解决网络覆盖和村村通问题。二是加快宽带网络优化升级。同步提升骨干网、接入网和网站等多个关键环节的网络能力。三是提高宽带网络应用水平。从经济发展、社会民生、文化建设、应用普及等方面深化宽带应用。四是促进宽带网络产业链不断完善。通过关键技术研发、重大产品产业化和支撑平台建设三个方面的重点工作,推进技术创新,提升产业自主能力。五是增强宽带网络安全保障能力。将宽带普及与保障安全相结合,同步加强宽带网络安全技术支撑能力建设,加快应急通信系统的宽带化改造,构建安全保障体系。为落实各项任务,《战略方案》以专栏的形式提出了“十二五”期间将组织实施的具有重大引导作用和示范意义的7项工程。

3. 政策措施

《战略方案》提出了一系列政策措施,确保实现我国宽带网络发展预期目标,主要内容包括7个方面:一是加强组织推动。国家发改委、工业和信息化部等相关部门将成立“宽带中国”战略实施协调小组,加强横向跨部委及纵向跨中央地方的组织协调,研究宽带发展中的重大问题。二是完善制度环境。完善法律法规,加强监管体系建设,推动开放竞争,深化应用创新。三是规范建设秩序。严格落实宽带网络建设规划和规范,保障宽带网络设施建设与通行,深化网络设施共建共享。四是加大财税支持,加快完善普遍服务补偿机制,促进提供

包括宽带在内的电信普遍服务，充分利用中央各类专项资金，支持农村和老少边穷地区宽带网络发展。五是规划频率资源。明确国家无线频谱路线图，促进频谱资源的高效利用，推动各种宽带技术发展。六是加强人才培养。创新宽带相关专业人才培养模式，优先保障人才发展投入，加大高层次宽带人才引进和培养。七是深化国际合作，不断提升我国宽带网络的国际地位。

（三）影响分析

宽带中国战略将对国家相关产业（如消费类电子产品、光纤、基础设施建设等）产生很大的拉动及提升作用，也将对信息消费产生强有力的支持与促进作用。

实施宽带中国战略，国家将加大对信息基础设施的投资力度，势必将加快以 4G 为代表的宽带通信技术等通信基础设施的建设和升级，城市及农村的带宽接入能力将得到大幅提升，进而助推信息消费发展。

宽带中国上升为国家意志，有利于促进三网融合。宽带基础设施是三网融合的物理基础，三网融合业务需要高带宽宽带网络的支撑。在三网融合的大趋势下，升级提速已是宽带发展的必然。加快宽带网络发展正式上升为国家战略意志，国家将进一步加大互联网基础设施建设，不断提高网络连接速度，推动互联网向高速互联网发展，势必促进三网融合。

三、信息安全政策高端化和常态化

（一）政策概况

《2006—2020 国家信息化发展战略》阐述了我国信息安全现状、问题、目标和任务，要求全面加强国家信息安全保障体系建设，大力增强国家信息安全保障能力。坚持积极防御、综合防范，探索和把握

信息化与信息安全的内在规律，主动应对信息安全挑战，实现信息化与信息安全协调发展。优化信息安全资源配置，建立和完善信息安全等级保护制度。加强密码技术的开发利用。建设网络信任体系。加强信息安全风险评估工作。建设和完善信息安全监控体系。高度重视信息安全应急处置工作。促进资源共享，重视灾难备份建设。积极跟踪、研究和掌握国际信息安全领域的先进理论、前沿技术和发展动态，掌握核心安全技术，提高关键设备装备能力，促进我国信息安全技术和产业的自主发展。不断提高信息安全的法律保障能力、基础支撑能力、网络舆论宣传的驾驭能力和我国在国际信息安全领域的影响力，建立和完善维护国家信息安全的长效机制。

2013 年 8 月 21 日，国家发改委、工业和信息化部、科学技术部、国家新闻出版广电总局四部委联合发布了《关于开展国家下一代互联网示范城市建设工作的通知》，要求建立重要网络应用安全评估制度，全面部署网络与信息安全防护体系，提高信息安全技术保障和支撑能力，加强网络信息与安全保障工作。

2013 年 11 月 12 日，党的第十八届中央委员会第三次全体会议通过的《中共中央关于全面深化改革若干重大问题的决定》提出，坚持积极利用、科学发展、依法管理、确保安全的方针，加大依法管理网络力度，加快完善互联网管理领导体制，确保国家网络和信息安全。设立国家安全委员会，完善国家安全体制和国家安全战略，确保国家安全。

（二）影响分析

国家层面提出完善互联网管理领导体制、设立国家安全委员会，完善国家安全体制和国家安全战略的总体部署和要求，将进一步加大依法管理网络力度，厘清相关监管部门的管理界面。促进网络与信息安全保障体系建设，特别是强化移动互联网、下一代互联网、云计算、

物联网、大数据等新兴技术业务的安全管理。

四、两化融合纵深推进

（一）政策概况

2009年10月21日，工业和信息化部印发《关于推进消费品工业两化融合的指导意见》，要求大力推进消费品工业“两化”融合。在专业信息服务工作方面，要求行业协会在政府指导下，及时反映行业“两化”融合情况、问题和建议，积极开展典型经验推广、行业“两化”融合发展水平评估、标准规范研究制定、人才队伍建设、技术和信息服务咨询等工作，促进“两化”融合有序开展。各类信息服务企业应不断提升自身能力，加快发展面向中小企业和专业市场的信息服务平台。鼓励消费品工业企业将信息技术服务外包。

2011年4月6日，工业和信息化部、科学技术部、财政部、商务部、国有资产监督管理委员会联合印发《关于加快推进信息化与工业化深度融合的若干意见》（工信部联信〔2011〕160号），提出八项主要任务及目标：到2015年，信息化与工业化深度融合取得重大突破，信息技术在企业生产经营和管理的主要领域、主要环节得到充分、有效应用，业务流程优化再造和产业链协同能力显著增强，重点骨干企业实现向综合集成应用的转变，研发设计创新能力、生产集约化和现代管理水平大幅度提升；生产性服务业领域信息技术应用进一步深化，信息技术集成应用水平成为领军企业核心竞争优势；支撑“两化”深度融合的信息产业创新发展能力和服务水平明显提高，应用成本显著下降，信息化成为新型工业化的重要特征。并提出了创新“两化”深度融合推进机制、加大财政资金和金融支持力度、组织广泛开展典型示范工作、加快发展和完善行业信息化服务体系、加强人才队伍建设和国际交流5项具体措施。

2013 年 9 月 5 日,工业和信息化部立足当前工作实际,针对制约工业转型升级的突出矛盾和问题,制定了《信息化和工业化深度融合专项行动计划(2013—2018 年)》(以下简称《两化融合专项行动计划》),提出了 8 项行动计划,务实推进两化融合重点工程,明确了推进两化深度融合的方向和突破口。

9 月 5 日,国家发改委、工业和信息化部等 14 个部门联合发布了《物联网专项行动计划》,为加快物联网基础设施建设、推动物联网在工业领域中的应用指明了方向。

目前,上海、广西等地正大力推进智慧工业园区建设。7 月,上海市经信委发布了《关于加快推进本市智慧园区建设的指导意见》,以信息基础设施优化、开发管理精细化、功能服务专业化、产业发展智能化为建设目标,力争到“十二五”期末,建设 8~10 个公用信息通信网络高速泛在、精细管理高效惠企、功能应用高度集成、智慧产业高端集聚的示范性智慧园区。8 月,广西发布了《广西推进实施两化深度融合专项行动方案》,提出未来 2~3 年打造一批两化融合示范智慧工业园区。截至 6 月底,全国 106 个国家级高新区中有 34 个正在推进智慧园区建设。

(二) 影响分析

两化融合纵深推进,各地落实信息消费政策和两化融合专项行动配套措施将大量实施,工业信息化基础设施水平将进一步提升。《两化融合专项行动计划》的实施也将促进更多省份探索开展地市一级两化融合水平评估。

移动互联网、大数据、云计算等新技术不断融入研发设计、生产制造、经营管理等环节,不断创新制造业信息技术集成应用模式和信息化服务模式。两化融合纵深推进,越来越多的工业企业将借助互联

网平台整合业务和服务体系，不断促进工业信息化领域业务应用技术和产品的推陈出新。

五、积极探索上海自贸区政策

中国（上海）自由贸易试验区 [China (Shanghai) Pilot Free Trade Zone] 简称上海自由贸易区或上海自贸区，是中国大陆境内第一个自由贸易区，将为上海带来十年发展红利。2013年8月，国务院正式批准设立中国（上海）自由贸易试验区，实行政府职能转变、金融制度、贸易服务、外商投资和税收政策等多项改革措施，将大力推动上海市转口、离岸业务的发展。

（一）出台背景

6月28日，上海市政府修正总体方案交各部委。7月3日，国务院正式通过上海自贸区方案。8月16日，上海自贸区暂停实施部分法律规定。8月27日，上海自贸区破冰式制度改革启动。9月18日，38家跨国公司地区总部落户自贸区。9月22日，工商银行自贸区支行悄然挂牌。9月24日，外高桥保税区上海自贸区初露脸。9月25日，上海市副市长艾宝俊兼自贸区主任。9月26日，上海在自贸区内调整地方性法规。9月27日，国务院印发上海自贸区总体方案。9月29日，上海自贸区正式挂牌成立。

为解决有关法律规定在试验区内的实施问题，十二届全国人民代表大会常务委员会第四次会议26日审议了《关于授权国务院在中国（上海）自由贸易试验区等国务院决定的试验区内暂时停止实施有关法律规定的决定（草案）》。在试验区内，对负面清单之外的外商投资暂时停止实施《外资企业法》、《中外合资经营企业法》、《中外合作经营企业法》3部法律的有关规定，暂时停止实施文物保护法的有关规定。在试验区内对外商投资试行准入前国民待遇，同时制订试验区内

外商投资与国民待遇等不符的负面清单，对负面清单之外的领域，将外商投资企业合同章程审批改为备案管理。方案还提出，允许符合条件的外商独资或中外合资、中外合作拍卖企业在试验区内从事文物拍卖业务，其文物拍卖资质申请及拍卖标的审核工作纳入现行管理体制。

为贯彻落实《国务院办公厅关于金融支持经济结构调整和转型升级的指导意见》，上海出台 42 条实施意见。实施意见明确提出上海要结合中国（上海）自由贸易试验区建设的要求，争取先行先试，使国家金融改革、创新有关部署在上海最先落地。

（二）政策概况

依据国务院通过的《中国（上海）自由贸易试验区总体方案》，上海自贸区将有以下规划与政策：先行试点人民币资本项目开放及逐步实现可自由兑换等金融措施，并采用循序渐进的开放政策，优先开放企业法人的人民币自由兑换；上海自贸区也有望成为中国加入“泛太平洋伙伴关系协议”（TPP）的首个对外开放窗口，为中国加入该协议发挥重要作用。该方案最终将可能落实到金融、贸易、航运等 5 个领域的开放政策，以及管理、税收、法规等 5 个方面的改革措施。此外，在金融领域，上海自贸区还将实现利率市场化、汇率自由汇兑、金融业的对外开放、产品创新等，也涉及一些离岸业务；在贸易领域，上海自贸区将实现“国境线放开”、“国内市场分界线安全高效管住”、“区内货物自由流动”的监管服务新模式，这是上海自贸区与目前上海综合保税区的主要区别。上海自贸区内 7 家银行已经开始试点几乎等同离岸账户的 FTA 账户。

上海自贸区所规划的主要扩大对外开放的政策如下。

1. 金融、航运与商贸领域

金融领域的政策主要有：允许符合条件的外资金融机构设立外资银

行，符合条件的民营资本与外资金融机构共同设立中外合资银行。在条件具备时，适时在试验区内试点设立有限牌照银行。在完善监管的同时，允许自贸区内符合条件的中资银行开办离岸业务；试点设立外资专业健康医疗保险机构；融资租赁公司在试验区内设立的单机、单船子公司不设最低注册资本限制；允许融资租赁公司兼营与主营业务有关的商业保理业务。上海自贸区执行宽进严管的管理思路，在自贸区内，1元钱就可以创办公司且大大简化审批手续，一般1天就能完成申办材料的审批，但若发生违法行为将受到诸多限制。在船舶航运方面，上海自贸区亦有大幅开放政策出台，主要包括：中外合资、中外合作国际船舶运输企业的外资股份比例限制被放宽，国务院交通运输主管部门将制定相关的规定加以有效管理；中国大陆资产的公司可以拥有或控股拥有不悬挂五星红旗的船舶，对外贸进出口集装箱在国内沿海港口和上海港之间的沿海捎带业务执行先行先试。商贸领域政策主要有：允许外资企业经营特定形式的部分增值电信业务，允许外资企业从事游戏游艺设备的生产和销售，通过文化主管部门内容审查的游戏游艺设备可面向国内市场销售。

2. 专业领域

允许设立外商投资资信调查公司；允许在试验区内注册的符合条件的中外合资旅行社，从事出境旅游业务（中国台湾地区除外）；外资方可以拥有不超过70%的股权的方式设立中外合资人才中介机构；港澳投资方可设立独资人才中介机构；外资人才中介机构最低注册资本金要求由30万美元降低至12.5万美元；自贸区内，取消上海市提供服务的外资工程设计（不包括工程勘察）企业的“首次申请资质时对投资者的工程设计业绩”之要求；自贸区内的外商独资建筑企业承揽上海市的中外联合建设项目，取消过去建设项目中外方投资比例限制。

3. 文化与社会服务领域

取消外资演出经纪机构的股比限制，允许设立外商独资演出经纪机构，为上海市提供服务；允许设立外商独资的娱乐场所，在试验区内提供服务；允许举办中外合作经营性教育培训机构；允许举办中外合作经营性职业技能培训机构；允许设立外商独资医疗机构。

在开启多项改革措施的同时，中国政府也对一些投资项目进行了限制。例如，音像制品和电子出版物、博彩、互联网等服务，政府均禁止或限制提供这些商品的外商进驻。另外，在自贸区挂牌的同时，官方也公告列明了《中国（上海）自由贸易试验区外商投资准入特别管理措施（负面清单，2013 年）》，对采矿、制造、建筑和批发零售等 18 个行业的部分内容进行了准入限制，其中博彩、网吧等属于禁止内容。中国海关也会加大监管力度，防止自贸区内可能出现的走私和其他违法行为。

（三）影响分析

上海自贸区正式挂牌成立前后均引起了各方高度关注，引发多家知名企业抢先入驻自贸区。上海自贸区的设立还将使上海的港口、机场、仓储、地产以及金融服务等行业获益，并大幅促进上海的离岸经济、港口经济和总部经济的发展，同时给长江三角洲地区的经济发展以正面辐射效应。

上海自贸区将会进一步促进电信业的改革发展。在自贸区将会允许外资企业突破之前股权比例低于 50% 的限制，甚至可能会允许外资企业以独资形式经营，但涉及信息安全的仍要严格审查。外国企业可以在自贸区内设置增值电信企业，但不限于在自贸区内开展业务，还可以经营全国性的增值电信业务，只是总部设在自贸区。

第三篇

区域篇



近年来,以促进信息化、个人信息保护、电信设施保护、计算机安全等为重点,全国各主要地区进行了互联网立法的探索。

第七章 北京市

一、推动信息化条例出台

北京市人民代表大会常务委员会于2007年9月在北京市第十二届人民代表大会常务委员会第三十八次会议上通过了《北京市信息化促进条例》,在信息化工程建设、信息资源开发利用、信息技术推广应用及信息安全保障等方面,为北京市属单位和企业制定了标准,并为违反上述领域规定的市属单位和企业制定了具体的罚则。

二、打击网络谣言

北京市人民政府新闻办公室、市公安局、市通信管理局和市互联网信息办公室共同研究制定了《北京市微博客发展管理若干规定》(以下简称《规定》),于2011年12月16日正式公布施行。首先,《规定》以“科学发展、积极利用、加强管理、确保安全”为指导原则,根据《中华人民共和国电信条例》、《互联网信息服务管理办法》等法律、法规、规章,结合北京市实际,就微博客建设、运用和管理作出十六条规定^①。其次,《规定》明确提出要加强微博客的建设、运用,发挥微博客服务社会的积极作用。网站从事微博客服务,应当坚持诚信办网、文明办网,积极传播社会主义核心价值观体系,传播社会主义先进文化,为构建社会主义和谐社会服务。再次,《规定》对北京市行政区域内

^① 包括目的依据、适用范围、发展原则、规划审批、行为规范、微博客用户注册、信息内容审核、政府部门责任、行业自律、社会监督、法律责任等内容。

网站开展微博客服务的申请程序和准入条件作出明确规定，基于保护用户利益和构建网络诚信体系，提出任何组织或者个人注册微博客账号，应当使用真实身份信息。最后，《规定》指出网站开展微博客服务，应当保证注册用户信息真实。《规定》依据国家法律法规，提出不得利用微博客制作、复制、发布、传播的十一类违法和不良信息，提出开展微博客服务的网站，要履行信息审核和监管职责，承担有关法律责任。

三、提高网络与信息安全事件突发应急能力

2013年2月1日，为进一步健全北京市网络与信息安全保障工作机制，提高应对网络与信息安全突发事件的能力，预防和减少突发事件造成的损失和危害，北京市通信保障和信息安全应急指挥部办公室依据《中华人民共和国突发事件应对法》、《北京市实施〈中华人民共和国突发事件应对法〉办法》、《北京市信息化促进条例》等法律法规，以及《国家突发公共事件总体应急预案》、《国家网络与信息安全事件应急预案》、《北京市突发事件总体应急预案》等相关规定，对2009年所发布的《北京市网络与信息安全事件应急预案》进行了修订。

此次修订在总结以往突发事件应对工作经验的基础上，进一步明确了预案的适用范围、组织机构及职责，细化了突发事件分级标准，完善了网络与信息安全预案体系建设和突发事件应对处置流程，使预案更具实操性，确保突发事件应对处置工作高效有序。预案修订后主要包括总则、组织机构与职责、监测预警、应急响应、恢复重建、保障措施、宣传、培训和演练等内容。

四、首提保护“网络安宁权”

2013年12月6日，北京市一中法院（以下简称“市一中院”）发布首个网络侵权案件权威调研报告，首次针对骚扰信息、垃圾邮件提出了

对网络安宁权要进行保护的新概念。有法官表示，目前立法方面还没有网络安宁权的规定，但是可以通过对人格权扩大解释给予保护，如果互联网用户认为过分的垃圾邮件、骚扰信息干扰了自己的正常生活并造成严重后果，可以通过诉讼的方式维护自己的权利。市一中院的调研称，在我国已经成为网民数量第一大国的背景下，借助网络平台和网络传播方式的侵权案件正快速增加。近3年来，市一中院共审理各类涉网络侵权案件200余件，其中2010年审结该类案件38件，2011年46件，2012年75件，2013年上半年已有50余件。在各类网络侵权的案件中，侵犯他人名誉权、肖像权、隐私权、姓名权等人格权的案件尤为突出。

市一中院经过对上述案件分析发现，网络侵权案件呈现出六大特征。除在网上晒他人私密照侵犯他人隐私权，借助网络平台造谣诽谤，谩骂侮辱侵犯他人名誉权等传统侵权模式之外，垃圾短信、骚扰邮件等新型侵权案件也逐渐增多。

对此，市一中院首次提出要对网络安宁权进行保护。该意见已通过立法建议的方式呈报最高人民法院和北京市高级人民法院。

五、加强舆论引导和互联网建设

2013年1月18日，在北京市召开的宣传部长会议上，市委常委、宣传部长、副市长鲁炜提出，2013年北京市宣传工作的重点之一就是建好互联网，制定实施北京互联网发展行动计划，发挥网络正能量。对于突发事件新闻报道和舆论引导，要做好专项新闻应急预案，依照全国人民代表大会常务委员会《关于加强网络信息保护的决定》推进网络真实身份管理。北京市即将出台以手机实名制为主要内容的《北京市移动电话信息服务管理若干规定》，强化微博客、社交网络、手机报等管理。同时，强调要建好、用好、管好互联网，主动抢占新媒体阵地，让正确的声音多发声，牢牢掌握网上话语权。此外，相关单位将开通官方微博、微信，多与读者、观众、听众进行互动，传递主

流信息。

六、确保互联网信息内容安全

新浪、搜狐、网易、百度、中搜、中国雅虎、奇虎七家搜索引擎服务商于 2009 年 12 月在北京网络新闻信息评议会第九次会议上签署了自律公约。公约中有“不以任何方式主动传播、收录、链接含有淫秽、色情等违法和不良信息内容的网站、网页”；“不为含有淫秽、色情等违法和不良信息内容的网站、网页提供搜索导航、广告、排名、接入等任何形式的网络服务”；“采取有力的技术手段阻止违法和不良信息”等条款。近年来，互联网搜索引擎技术发展十分迅速，功能越来越强大，应用越来越广泛。尽管由于其技术特点很难做到不良信息百分百不收录、不链接，但不可否认的是，服务商的社会责任是否到位，经营方针是否正确，自律机制是否完善，在其中发挥着主导作用。

第八章 上海市

一、推动信息化条例出台

上海市人民代表大会常务委员会于2012年第87次会议上暂定将《上海市信息化条例（暂定）》加入2013年的立法计划中，2013年6月10日，上海市政府法制办向上海市律师协会征询了《上海市信息化条例（草案）》的修改意见，经由行政法业务研究委员会、信息网络与高新技术业务研究委员会组织征询委员意见后完成书面修改意见，由市律协于6月24日提交市政府法制办。最终修改意见共计31条，涉及立法目的、适用范围和基本原则、政府推动和信息化教育培训宣传、信息化发展规划编制、信息基础设施建设、信息技术应用推广、信息资源开发利用、信息工程项目管理、信息产业发展、信息安全保障等内容。

二、促进电子商务发展

2008年11月26日，上海市第十三届人民代表大会常务委员会第七次会议通过了《上海市促进电子商务发展规定》（以下简称《规定》），并于2009年3月1日正式生效。《规定》确定了优先支持的电子商务相关项目，包括：先进制造业和现代服务业等重点领域电子商务平台的建设，电子支付、安全认证、信用服务、物流信息等电子商务服务体系的建设和电子商务关键技术的研发和推广应用等。在政府采购方面，要求上海市政府采购应当优先采用电子化方式，利用相关电子商务平台，开展交易、支付、信用评估和信息发布等活动；创新电子签名和认证技术；推动建立适应电子商务发展的风险投资、融资担保等手段，

建立与电子商务相关的消费者权益保护机制。

三、推动互联网基础网络建设

为加快推进智慧城市建设，进一步加快上海市宽带城市和无线城市建设中的光纤宽带固网、无线局域网（WLAN）、移动通信基站等通信基础设施建设，上海市通信管理局于2013年3月25日下发了《关于新建住宅区和住宅建筑内通信配套交付使用许可规定的通知》，根据小区住户数的不同，确定了小区综合性电信中心机房的最小面积及相关设施的配套，规范了住宅建设方、设计单位、施工企业和电信运营企业的有关行为。

四、加强互联网新闻应急管理

上海市人民代表大会常务委员会于2012年9月12日举行《上海市实施〈中华人民共和国突发事件应对法〉办法（草案）》（以下简称《办法（草案）》）的法规解读会，遵循《办法（草案）》“有几条立几条”的立法思路，重在体现上海地方特色，创制了较多具有地方特色的条款，对电信运营企业参与和配合突发事件处置提出了具体要求。第二十七条规定，广播、电视、报刊等新闻媒体和互联网新闻信息服务单位、电信运营企业、公共场所电子显示屏管理单位，应当配合做好预警信息的发布工作。

五、拟立法推动网络个人信息保护

上海市人大代表呼吁加快立法打击网络犯罪，为遏制越来越泛滥的各类垃圾信息，保障公民个人信息安全，2013年“两会”期间，李飞康代表提出了《尽快制定严厉惩处电话诈骗、垃圾短信及垃圾传真之上海地方性法规细则》的建议。为此，有关政府部门积极贯彻国家规定，加大了对电话诈骗、发送垃圾短信等行为的打击力度，要求电

信运营企业通过智能分析，拦截有害信息的发送。上海市经信委负责人坦言，目前的法规对垃圾信息发送者没有处罚措施和制裁手段，相关实施细则缺位或者缺乏可操作性。为加强对个人信息的保护，从源头上防范电话诈骗和垃圾信息，近年来，上海市在地方立法方面已进行了一系列的初步探索，拟在《上海市信息化条例（草案）》中规定个人信息保护的相关内容。

第九章 广东省

一、推动信息化条例出台

广东省人民代表大会常务委员会于2012年5月出台了《广东省信息化促进条例（征求意见稿）》（以下简称《条例》），在广东省政府法制办官网公开征求意见。《条例》分信息安全保障、信息资源开发利用、信息化规划编制等十章65条，其中明确规定县级以上人民政府应当及时公布信息化发展专项规划及年度执行报告，接受社会监督和质询。省人民政府应当建立全省统一的信息资源共享交换平台，通过电子政务网络实现政务信息和基础信息资源在国家机构以及社会公共服务单位之间的共享使用。县级以上信息化行政主管部门应当会同有关单位，编制政务信息和基础信息资源共享交换目录，明确政务信息和基础信息资源共享的内容、方式、技术规范和责任，并根据职责分工开发政务信息和基础信息资源。

二、保障网络信息系统安全

广东省人民代表大会常务委员会根据《中华人民共和国计算机信息系统安全保护条例》，于2008年出台了《广东省计算机信息系统安全保护条例》，根据计算机信息系统在国家安全、经济建设、社会生活中的重要程度，计算机信息系统受到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素，将计算机信息系统安全保护等级分为五级，并针对不同等级，制定了不同的保护措施和安全要求。除此之外，还在第三章安全秩序中，对互联网经营场所的安全管理系统提出了要求，对接入互联网的计算机

提出了保密性要求，规定了公安机关、国家安全机关、保密工作部门、密码管理部门等机构的监督责任。

三、维护互联网信息内容安全

广东省通信管理局、广东省公安厅、广东省人民政府新闻办公室于2005年共同下发了第16号文件《关于进一步加强防范互联网上有害信息的通知》，对不同种类的互联网业务经营者应承担的责任进行了划分，要求网站接入服务提供者切实担起相应的监督和配合查处责任，进一步强化对网站许可或备案证明的核验工作，不得为未经许可或备案的网站提供互联网接入服务，并依照国家有关规定做好所接入用户信息动态管理、记录留存、有害信息报告等网络信息安全管理。对有关主管部门依法处以关闭处罚的网站，应当立即终止为其提供网站接入服务。

四、推动电信基础设施建设

广东省通信管理局根据工业和信息化部、国务院国有资产监督管理委员会《关于推进电信基础设施共建共享的紧急通知》，结合广东省的实际，于2008年12月制定了《广东省推进电信基础设施共建共享实施办法（试行）》，很好地落实了科学发展观以及建设资源节约型、环境友好型社会的需求，减少了电信重复建设，提高了电信基础设施利用率。

第十章 浙江省

一、推动信息化条例出台

浙江省人民代表大会常务委员会于2010年7月在浙江省第十一届人民代表大会常务委员会第十九次会议上通过了《浙江省信息化促进条例》，主要目的是加快信息化发展，规范信息化工作，推进信息化与工业化融合，促进经济发展和社会进步，所规范的领域包括信息化规划与建设、信息产业发展、信息技术推广应用、信息资源开发利用、信息安全保障及相关管理活动。《浙江省信息化促进条例》出台之前，为了促进高新技术及产业的发展，浙江省人大于2009年9月通过了《浙江省高新技术促进条例》，主要目的也是促进高新技术及其产业的发展，加快传统产业改造提升，推动经济转型升级。

二、加强通信计量监控

2013年7月26日，浙江省第十二届人民代表大会常务委员会第四次会议高票审议通过了《浙江省计量监督管理条例》，并于2014年1月1日起正式实施。为进一步加强计量监督管理，适应浙江经济社会发展对计量法制的要求，为民生计量提供坚实的法制保障，浙江省制订出台了《浙江省计量监督管理条例》，条例共七章51条，对计量单位和计量器具、计量检定和计量校准、贸易计量、计量监督检查、法律责任等方面作出了具体规定。

《浙江省计量监督管理条例》完善并强化了对民生计量的法制保障，对“民用四表”、电信的计时计价器、房产面积的测量器具强制检定等在法律层面进行了明确规定。特别是条例中“电信运营

商应当依法配备和使用经强制检定合格的电话计时计费装置，并按照检定周期向计量主管部门授权的计量检定机构申请检定”、“计量主管部门应当按照规定职责加强对电信运营商网络流量计量活动的监督管理”的规定，改变了过去通信计量由电信运营商自己说了算的格局，既能进一步保障通信计量的准确性，又能更好地维护群众权益。

三、提升宽带网络服务质量

为全面落实《“宽带中国”2013专项行动浙江省实施方案》，浙江省通信管理局于2013年4月25日下发了《关于开展宽带业务市场专项治理的通知》（以下简称《通知》），主要目的是进一步规范宽带业务市场行为，提高宽带网络质量和宽带服务水平，维护用户合法权益，推动全省信息化水平提升。《通知》确定了四个方面的工作内容：第一，自觉履行服务承诺，提高宽带服务水平；第二，提高实际接入速率，建立宽带速率测试机制，提升用户上网体验；第三，严格规范宽带业务市场行为，切实维护用户合法权益；第四，建立合理的宽带价格体系，积极推进宽带中国2013专项行动。

四、大力推进电子商务发展

2013年6月，浙江省工商行政管理局出台了《关于促进网络市场快速有序发展的若干意见》（以下简称《意见》），在便捷市场准入、网络市场冠省名、健全网络市场维权机制等方面给予网络市场进一步支持。

根据《意见》，工商部门将支持企业名称体现网络经济特征，鼓励网络市场主体名称体现行业特点，允许使用“电子商务”或表明其行业特点的各类新兴行业用语作为行业表述。在不违反企业名称登记管理相关规定的前提下，电子商务企业可以使用包括自有网站中文域

名在内的个性化词语作为企业名称的字号（商号）。

《意见》放宽了经营场地限制和经营范围。电子商务企业可以使用“网上经营××”或“网上提供××服务”等作为经营范围。对《国民经济行业分类》未包含的新兴网络经济行业，登记机关可以根据企业申请，参照《新兴行业企业登记试行意见》（企函字〔2012〕4号）的规定，依法灵活核定其经营范围。国家和地方政府批准设立的科技产业园区内设立的企业，可以凭园区管委会出具的住所使用证明，办理注册登记手续。

《意见》还规定，免征网络市场主体登记费。自2013年1月1日至2014年12月31日，免征各类网络市场主体注册登记费。

第十一章 其他地区

一、湖南省出台全国首部信息化地方性法规

2004年7月30日,《湖南省信息化条例》作为全国第一部信息化的地方性法规,在湖南省正式实施。随着经济社会加快发展和转型,信息化发展的环境、形式和任务都发生了较大的变化,迫切需要对原《条例》进行修订。2012年5月31日,湖南省第十一届人民代表大会常务委员会第二十九次会议审议通过了《条例》修订。修订后的《条例》共56条,从主体责任、规划编制、政策支持、行为规范、监督管理、法律责任6个方面,对原《条例》进行了补充和完善,其特色和亮点有:加强全省统筹规划,实行集约化建设和管理,从源头上防止重复建设;加快推进电信网、广播电视网、互联网在业务、网络和终端等层面的融合;商业开发建筑物内的信息管线和设施建设由建设单位负责建设,避免网络运营商的垄断;推进重大基础性信息资源的开发利用,推动政务信息的交换整合,资源共享;任何单位和个人不得非法披露所采集的信息,不得出售或者以其他方式非法向他人提供信息,不得以窃取等方式非法获取信息;从事信息技术产品制造、软件开发以及信息服务的,按规定享受税收减免、投资融资、土地使用、人才培养等方面的优惠政策,等等。

二、江苏省信息化条例明确规定个人信息保护

2011年9月20日,江苏省第十一届人民代表大会常务委员会第二十四次会议提交审议通过《江苏省信息化条例(草案修改稿)》。针对个人信息泄露、非法买卖等乱象,草案修改稿明文规定,任何单

位和个人不得将提供服务过程中获取的公民、法人和其他组织的信息，出售或者以其他方式非法提供他人，或者以窃取、购买等方式非法获取上述信息。否则，将追究相应的法律责任。条例规定，对于倒卖个人信息的单位，将处以十万元以上、最高五十万元的处罚。这是我国第一部明确规定个人信息保护的法规。尽管只是一部地方性法规，但在当时国家层面相关法律缺位的情况下，江苏省这一“首吃螃蟹”的动作，被认为具有“里程碑意义”。

三、山西省信息化条例严惩出售个人隐私行为

《山西省信息化促进条例》（以下简称《条例》）是山西省第一部规范信息化建设和管理的地方性法规，自2013年10月1日起施行。关于《条例》的特色规定，核心内容之一是推进两化深度融合，为此，山西省鼓励企业建立首席信息官制度，推进信息化与工业化的深度融合。此外，《条例》还是目前国内首部地方信息保护法规，第三章“信息资源共享与开发利用”详述了信息采集、共享和使用的原则，制定了具体的罚则。

《条例》中规定，非法获取信息，非法披露、非法出售或者以其他非法方式向他人提供所获取信息的，由公安机关责令停止违法行为，没收违法所得；对单位处十万元以上五十万元以下的罚款，对个人处一万元以上五万元以下的罚款；构成犯罪的，依法追究刑事责任。公民发现泄露个人身份、散布个人隐私等侵害其合法权益，或受到商业性电子信息侵扰的，有权要求服务提供者删除有关信息或者采取其他必要措施予以制止，同时可以向公安机关举报。这意味着，《条例》实施后，如市民再收到垃圾邮件，可要求服务商删除相关信息。

公民、法人和其他组织有权要求采集、使用其信息的单位和个人更正、删除与其相关的不实信息。山西省将加大公共信息服务，按要求，社会保障、环境保护、气象等部门，以及供电、供水、供气等与

民生息息相关的公共服务机构，应建立健全公共服务信息系统，及时、准确地提供与生活相关的公共信息服务。

四、海南省信息化条例强化信息网络和系统的监督管理

2013年9月，海南省第五届人民代表大会常务委员会第四次会议审议通过了《海南省信息化条例》，并于11月1日起施行。近年来，海南省在公共信息网络、电子政务、产业政策等方面相继出台了一系列政府规章和规范性文件，很好地促进了信息产业的发展，但同时也产生了一些新问题，如信息化统筹协调的组织体制不健全；信息系统建设缺乏统筹规划和资源共享，重复建设较为严重；信息化工程质量和进度缺乏监督考核；安全基础设施建设、技术保障措施薄弱，网络和信息安全问题较为突出等。为提高信息安全保障能力和水平，维护公众利益和国家安全，《条例》第五章对建立信息安全保障体系、实行信息安全等级保护、信息安全风险评估、信息安全事件应急预案、网络身份认证等方面作出了规定。第六章设专章明确了信息化主管部门、公安机关、国家安全机关、电信管理机构等的监督职责，提出加强信息资产的管理，建立信息资产使用评估制度，促进信息资源的优化配置。

五、辽宁省修订计算机信息系统安全管理条例

新修订的《辽宁省计算机信息系统安全管理条例》于2013年9月23日获得通过。

新修订的条例规定，任何单位和个人不得利用信息系统制作、复制、发布和传播下列信息：反对宪法确定的基本原则的；危害国家安全、泄露国家秘密，颠覆国家政权、破坏国家统一的；损害国家荣誉和利益的；煽动民族仇恨、民族歧视，破坏民族团结的；破坏国家宗教政策，宣扬邪教、封建迷信的；散布谣言，煽动非法聚集，扰乱社会秩序，

破坏社会稳定的；宣扬淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪，或者交易、制造违禁品、管制物品的；侮辱或者诽谤他人，侵害他人合法权益的；法律法规禁止的其他内容。

新修订的条例指出，单位和个人利用信息系统制作、复制、发布、传播上述内容，由公安机关予以警告，情节严重的，责令六个月以下停止联网、停机整顿，必要时依法吊销经营许可证或取消相关资格；构成治安管理处罚的，依照《中华人民共和国治安管理处罚法》的规定处罚；构成犯罪的，依法追究刑事责任。

此外，互联网服务提供者和互联网使用单位应当建立信息审核制度，明确审核人员，发现违法信息，应当先行保存有关记录，及时采取删除、停止传输等处置措施，并向公安机关等有关部门报告。

对于非法入侵的“黑客”故意传播计算机病毒的行为，公安机关可处以 1000 元以上 5000 元以下罚款。

六、重庆市推举措促消费增长

2013 年 7 月，重庆市商业委员会确定六项举措稳定下半年消费增长，提出宣传贯彻好市政府《关于促进网络零售产业加快发展的意见》，编制网络零售产业发展规划及工作方案，抓好网络零售“千亿级产业”布局落地以及电子商务企业的引进和传统企业上线培育工作。

除此之外，其他举措包括举办各类餐饮美食促销活动；抓好商圈业态调整和规划布局、打造主城智慧商圈、推进中央商务区和便民商圈建设；培育品牌展会；清理整顿大型商贸企业向供应商违规收费工作，加强单用途商业预付卡管理；抓好市场供应，建设完善城乡统筹的商贸网络体系和整顿规范市场经济秩序的长效机制，着力打造会展之都、购物之都、美食之都。

七、黑龙江省制定《移动智能终端服务公开承诺》

截至2013年3月底，黑龙江省移动互联网用户数达1870万户，占手机用户总数的65%以上。在移动互联网用户数快速增长的同时，服务、安全、收费等侵害消费者权益的问题也逐渐凸显。这不仅侵害了消费者的合法权益，也给整个行业带来了不良影响。为此，黑龙江省移动互联网产业联盟的二十家单位共同制定了《黑龙江省移动智能终端服务公开承诺》，共九条内容，承诺以诚实守信、明码实价、规范促销、不预置恶意应用软件、售后服务严格执行国家标准，自觉规范移动智能终端服务行为，认真接受广大消费者的监督。由于成员单位覆盖了黑龙江省主要的移动智能终端市场，此公开承诺的对外公示，必将对提高黑龙江省移动智能终端服务的质量发挥良好作用。

八、山东省全面推动网络经济发展

2013年8月9日，网络商品交易监管一直走在全国前列的山东省出台《关于促进全省网络经济健康快速发展的若干意见》（以下简称《意见》），加大对网络经营者的扶持、服务和监管力度，促进网络经济和实体经济融合发展。

《意见》共分4个方面27条措施。根据《意见》，山东省将放宽市场准入，大力培育发展网络经营主体。自然人通过第三方网络交易平台开办网店，经营项目不涉及前置审批的，经交易平台实名制审查后，即可开展经营活动。具备登记注册条件的，依法办理工商登记注册，工商部门将放宽企业名称登记、企业住所登记、经营范围登记等方面的限制。

《意见》还支持实体经济转型升级，推进实体经营向网上经营延伸。大力支持发展现代物流业，为网络经济快速发展提供物流支持。大力培育网络交易平台，发展一批行业集聚性强、专业特色明显、功能齐

全的交易平台；支持发展网上商品交易市场，推动传统市场转型升级。

《意见》表示，工商部门将充分运用信息化手段，提高对网络经营者监管服务效能，如引导实施商标战略，培育一批网络经营品牌，规范网络经营签约行为，帮助网络经营企业拓宽融资渠道等，并强化监督管理，切实规范网络交易秩序。

九、郑州市互联网业承诺保护公民个人隐私

2013年7月19日，郑州市互联网信息办公室组织属地网络界认真学习《全国人民代表大会常务委员会关于加强网络信息保护的決定》，并就保护公民个人隐私作出公开承诺。中原网、郑州广播在线、郑州教育信息网等属地重点网站提出要切实增强网站工作人员对保护公民个人隐私重要性的认识，并就保护公民个人隐私作出公开承诺。

据中原网相关负责人介绍，中原网微博、论坛等用户个人真实注册资料通过公安部门数据库验证并保存，工作人员无法进行查看。用户操作日志等内容只有接到司法部门明确要求才能调阅查看。同时通过客服电话、邮箱等多种渠道接受用户就个人隐私保护方面的投诉，及时帮助用户处理。

三大电信运营商和景安网络公司针对接入的网站采取增加屏蔽关键词、提高人工巡视线上内容频率、封禁违规用户、公司专人配有专有限、客户资料必须经执法人员出示协查函才可以查阅等有针对性的管理措施，利用机器和人工结合的办法有效进行个人隐私保护。

第四篇

专题篇



第十二章 互联网金融创新

一、概述

2013年6月13日,余额宝作为第三方支付平台支付宝打造的一项余额增值服务,上线存款业务。用户在支付宝网站内就可以直接购买基金等理财产品,获得相对较高的收益,同时余额宝内的资金还能随时用于网上购物、支付宝转账等支付功能。转入余额宝的资金在第二个工作日由基金公司进行份额确认,对已确认的份额会开始计算收益。截至2013年11月14日15:00,天弘增利宝货币基金(余额宝)的规模突破1000亿元,用户数近3000万户,天弘增利宝成为国内基金史上首只规模突破千亿元关口的基金,在全球货币基金中排名第51位。

余额宝推出之后,腾讯、百度等在互联网金融领域也有相应动作。2013年8月5日,微信支付上线,微信支付是腾讯公司移动社交通信软件微信与第三方支付平台财付通联合推出的移动支付创新产品,旨在为广大微信用户及商户提供更优质的支付服务,其支付和安全系统由腾讯财付通提供支持。除了牵手包括华夏在内的多家基金公司外,微信支付还将引入银行理财产品。8月底,百度悄然上线了百度金融测试版,意在争夺金融产品搜索入口。10月21日,百度宣布“百度金融中心——理财”平台将于10月28日正式上线,并携手华夏基金推出年化收益率8%的理财计划“百发”,限量发售10亿份。但该业务随后被证监会叫停,原因是百度联合华夏基金推出的理财计划“目标年化收益率8%”不符合《基金法》等规定的“公开披露基金信息不得有预测投资业绩”等要求,证监会将根据百度及相关机构报送的书面材料,对该业务合规性予以核查。压力之下,百度改口称,并未承诺保本保

收益，8%的收益率仅是目标。在首款理财产品上线界面上，百度已改变宣传口径，将“目标年化收益率为8%”等收益预期相关字句撤下。12月6日，京东正式上线名为“京保贝”的“3分钟融资到账”业务，这是一款由京东商城推出的创新型快速融资业务，京东的上万家供应商均可凭采购、销售等数据快速获得融资，融资成本约为10%。这也是继2012年推出供应链融资业务以来，京东推出的又一项创新型快速融资业务。

不仅如此，余额宝的出现催生了“互联网金融”发展的新热潮，使互联网金融成为2013年互联网行业发展的“关键词”。互联网金融的创新模式不断推陈出新。网络小贷、网络众筹、P2P、比特币等互联网金融脱媒模式蓬勃发展。2013年10月，由阿里巴巴掌门人马云、中国平安董事长马明哲和腾讯科技董事长马化腾联手创立的众安在线财产保险股份有限公司已获得保监会的审核验收，国内首家互联网保险公司获批开业。

总结起来，互联网金融的类型包括：一是基于第三方支付的金融产品销售和结算，如余额宝；二是基于交易信息的小微信用贷款，如阿里小贷；三是基于信息平台的融资服务，如P2P网络借贷和网络众筹；四是基于软件系统和密码学的虚拟货币，如比特币等。

P2P网络借贷是P2P借贷与网络借贷相结合的金融服务模式。P2P借贷是个人对个人的借贷，借贷过程中，资料与资金、合同、手续等全部通过网络实现。P2P网络借贷平台则是提供前述服务的平台。P2P网络借贷是随着互联网的发展和民间借贷的兴起而发展起来的一种新的金融模式。

网络众筹是指以团购+预购的形式，向网友募集项目资金的模式。众筹利用互联网和社交网络传播的特性，让小企业、艺术家或个人对公众展示他们的创意，争取大家的关注和支持，进而获得所需要的资金援助。

比特币（Bitcoin）是一种由开源的 P2P 软件产生的数字货币。最初由中本聪（Satoshi Nakamoto）提出理念，以开放、对等、共识、直接参与的理念为基准，结合开源软件和密码学中块密码的工作模式，在 P2P 对等网络和分布式数据库的平台上，开发出比特币发行、交易和账户管理的操作系统。比特币与其他虚拟货币最大的不同，是其不依赖中央银行、政府、企业的支持或者信用担保，而是依赖对等网络中种子文件达成的网络协议，去中心化、自我完善的货币体制，理论上确保了任何人、机构或政府都不可能操控比特币的货币总量，或者制造通货膨胀，且其总数量是非常有限的，具有极强的稀缺性。该货币系统在前 4 年内只有不超过 1050 万个，之后的总数量将被永久限制在 2100 万个之内。为此，比特币在全球掀起投资高潮，交易价格不断上涨，国内的最高成交价在 2013 年 11 月 29 日产生，为 7499 元 / 个。但在多个国家推出管制措施之后，比特币的交易受到影响，价格回落。此外，还有支持比特币支付的网店、取款机等，以及基于比特币技术原理的“山寨币”。

二、法律分析

互联网金融服务归根结底是一种金融服务，现有的法律已经能够基本覆盖，如《合同法》、《证券法》、《贷款通则》等。但对于网络借贷、众筹、比特币等基于互联网特点产生的新的业务形态，在法律上，要与非法集资、非法吸收公众存款等相区分，并防范相应的法律风险。

对于网络借贷，根据《最高人民法院关于人民法院审理借贷案件的若干意见》的规定，自然人之间、自然人与法人、自然人与其他组织之间的借款作为借贷案件受理，确保了民间借贷的组织形式及其合法性。《合同法》第二百一十一条：“自然人之间的借款合同约定支付利息的，借款的利率不得违反国家有关限制借款利率的规定。”《最

高人民法院关于人民法院审理借贷案件的若干意见》：“六、民间借贷的利息可适当高于银行利率，但最高不得超过同期银行贷款利率的4倍，超出部分的利息法律不予保护。”因此，若故意以高利率吸引他人出借款项并将资金用于套利的或者以欺骗手段骗取他人出借款项的，将构成犯罪，要追究相应的刑事责任。据统计，2007年以来，全国P2P借贷网站累计2000多家。截至2012年年末尚存300余家，贷款余额超过200亿元，借出人规模超过5万人。虽然交易总体规模较小，但年增长率超过500%。在网络P2P发展过程中，已发生诸多的法律问题，例如，多家网络P2P公司出现创始人卷款逃离、风险失控、业务违规整改等各种原因导致倒闭或停止业务开展。网贷公司也存在信用风险，由于资金流量规模较小，多数银行并不给予P2P网贷公司资金托管服务，这便给部分恶意创办的网贷平台提供了利用管理不严的资金托管机构进行欺诈的机会。为解决上述问题，2013年11月25日，在由银监会牵头的九部委处置非法集资部际联席会议上，网络借贷与民间借贷、农业专业合作社、私募股权领域非法集资等一同被列为须高度关注的六大风险领域。人民银行条法司相关人士给出了明确的风险警示，要求明确P2P网络借贷平台的业务经营红线。央行对“以开展P2P网络借贷业务为名实施非法集资行为”作了较为清晰的界定：第一类为当前相当普遍的理财—资金池模式；第二类为不合格借款人导致的非法集资风险；第三类则是典型的庞氏骗局。央行提出的方案是，建立平台资金第三方托管机制。应当在鼓励P2P网络借贷平台创新发展的同时，合理设定其业务边界，画出红线，明确平台的中介性质，明确平台本身不得提供担保，不得归集资金搞资金池，不得非法吸收公众存款，更不能实施集资诈骗。2013年12月，上海市网络信贷服务业企业联盟发布了《网络信贷行业准入标准》，这是网贷行业的全国首个行业标准，不仅涉及资金的第三方存管、清结算分离、风险管理制度、定期信息披露、出借人利益保护，更对注册资本、任职资格、从业人员备案等进行了详细限制。

对于网络众筹，在法律上，首先最应防范的是众筹演变为非法集资的风险。众筹模式中所有的项目不能够以股权或是资金作为回报，项目发起人更不能向支持者许诺任何资金上的收益，必须是以实物、服务或者媒体内容等作为回报，对一个项目的支持属于购买行为，而不是投资行为。其次是公开发行，众筹模式出资人众多，动辄达到数百乃至上千人；根据法律规定，募资对象超过 200 人即为公开发行。

关于比特币，12 月 5 日，央行等五部委发布《关于防范比特币风险的通知》（以下简称《通知》），《通知》明确了比特币的性质，认为比特币不是由货币当局发行，不具有法偿性与强制性等货币属性，并不是真正意义上的货币。同时，从性质上看，比特币是一种特定的虚拟商品，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。但是，比特币交易作为一种互联网上的商品买卖行为，普通民众在自担风险的前提下拥有参与的自由。《通知》要求，现阶段，各金融机构和支付机构不得以比特币为产品或服务定价，不得买卖或作为中央对手买卖比特币，不得承保与比特币相关的保险业务或将比特币纳入保险责任范围，不得直接或间接为客户提供其他与比特币相关的服务，包括：为客户提供比特币登记、交易、清算、结算等服务；接受比特币或以比特币作为支付结算工具；开展比特币与人民币及外币的兑换服务；开展比特币的存储、托管、抵押等业务；发行与比特币相关的金融产品；将比特币作为信托、基金等投资的投资标的等。《通知》规定，作为比特币主要交易平台的比特币互联网站，应当根据《中华人民共和国电信条例》和《互联网信息服务管理办法》的规定，依法在电信管理机构备案。同时，针对比特币具有较高的洗钱风险和被犯罪分子利用的风险，《通知》要求相关机构按照《中华人民共和国反洗钱法》的要求，切实履行客户身份识别、可疑交易报告等法定反洗钱义务，切实防范与比特币相关的洗钱风险。

三、国外立法与借鉴

在美国，P2P 网络借贷受到证券相关法律的规范。而在网络众筹领域，根据《创业企业扶助法案》，美国证券交易委员会专门出台了众筹的规则，寻求融资的创业者和初创企业将可以通过互联网向普通公众征集小规模投资。美国证券交易委员会（SEC）在当地时间 10 月 23 日推出了备受关注的“众筹”规则。根据这项法规，寻求融资的创业者和初创企业将可以通过互联网向普通公众征集小规模投资。在“众筹”规则生效后，美国创业公司可以向普通公众征集小规模投资。普通投资者将可审阅这些公司的业务发展计划，并选择其中前途较好的公司来进行投资。根据《创业企业扶助法案》的规定，SEC 必须对自己的法规作出改动，允许公司每年可通过“众筹”网站筹集最多 100 万美元资金。就目前而言，如果一家公司没有事先向 SEC 登记，那么就不得通过发行新股的方式来筹集资金。有支持者认为，股票“众筹”规则将可为那些被风险投资家忽视的公司提供新的资本来源，这些公司经常都会由于规模过小而不被重视。

对于比特币，各国有不同的法律规定。针对虚拟货币可能对美国联邦政府及整个社会带来的风险和前景，美国考虑对比特币进行立法。美国财政部下属的一个部门 2013 年 3 月曾表示，所有交换和转账虚拟货币的公司都应该被看成“金融服务业务”，这意味着这些公司必须向政府提供信息并且采取一些政策防止洗钱，这同时也会给那些与不遵守规则的公司做生意的金融机构带来风险。2013 年 8 月，美国得克萨斯州法官在审判关于特兰顿·谢沃斯（Trendon Shavers）比特币的虚拟对冲基金（Bitcoin Savings and Trust, BTCST）的案件中裁定：比特币是一种须遵守美国相关法律的货币形式。

2013 年 6 月底，德国议会决定持有比特币一年以上将予以免税，比特币被德国财政部认定为“记账单位”，这意味着比特币在德国已

被视为合法货币，并且可以用来交税和从事贸易活动。

2013年7月30日，泰国比特币创业公司 Bitcoin Co 表示，由于泰国央行封杀了比特币，因此该公司将停止所有业务。泰国外汇管理和政策部的高官表示，由于目前缺乏适用的法律和资本管制措施，加之比特币跨越多种金融业务，因此下述比特币活动在泰国都被视为非法：买卖比特币、用比特币买卖任何商品或服务、与泰国境外的任何人存在比特币的往来。

2013年12月3日，荷兰央行也发表声明质疑比特币，称其存储无安全保证，没有中央发行者对之负责，以及比特币价格存在极大的波动性。华尔街金融博客 zerohedge 网站发表评论称，荷兰央行的这份声明在竭力提醒比特币的潜在用户或交易者，这种货币具有“邪恶”的一面。

2013年12月5日，法国中央银行发布消息，警告比特币存在风险。法国银行称，比特币兑换法定货币的价格，存在天然的不稳定性，持有者或发现，很难将比特币兑换为现实货币。比特币的匿名性，还将为洗钱和恐怖主义集资等非法活动提供便利。法国银行还表示：“目前，比特币不是一种可信的投资渠道，并没有对金融稳定性造成实质影响。但是，比特币对持有者确实构成了风险。”法国银行警告，比特币兑换实体货币的不确定性，或导致商家竹篮打水一场空。

韩国金融当局于2013年12月12日宣布比特币缺乏稳定性，因此并不拥有“固有价值”，同时，对比特币缺少可测量的金融结构和指标表示担忧。韩国虽未否认比特币的合法性，但金融当局已承诺要加强对虚拟货币贸易，尤其是对洗钱活动以及其他违法活动的监管。

从国外的立法实践可以看出，面对互联网金融创新，各国的态度不一，但总体上互联网金融服务应遵守原有的金融法律规则，并防范其模式创新带来的新的法律风险。

四、总结和评述

互联网金融,其本质仍是“金融”,互联网是作为金融的工具,因此,应适用金融行业的相关法律法规。但不可否认的是,P2P网络借贷、网络众筹等新兴业务不断涌现,业务形式多种多样、业务流程差别较大、盈利方式也不尽相同,无法轻易归类到已有的金融业务分类中,对传统金融监管和法律带来了新的挑战。信用风险、非法集资、洗钱、金融诈骗等在互联网金融模式下又有了新的体现方式,需要进行立法和规范。

第十三章 “3·15 晚会”关注个人信息保护问题

一、概述

2013 年“3·15 晚会”对当今互联网技术 Cookie 进行了“曝光”，称收集用户行为的 Cookie 侵犯用户隐私，引起了社会各界对于 Cookie 信息使用 and 用户个人信息保护的广泛探讨。我们知道，一方面，我国的个人信息保护立法刚刚起步，“3·15 晚会”之时工业和信息化部《个人信息保护规定》尚未出台，很多问题没在法律层面上得以解决；另一方面，Cookie 是中立的技术工具，既能带给用户便捷，也涉及用户对于个人信息的掌控权，此二者是矛盾还是可以兼顾，也值得探讨。

Cookie 技术的使用最初是为了给用户带来便捷。用户浏览网站时会在网站留下 Cookie 数据，一般被用来存储用户的浏览记录、IP 地址、网卡号、用户名、密码等信息，可以省却用户再次登录网站时输入用户名和密码的步骤。一般情况下，Cookie 数据存放于用户电脑中，且每个网站对应各自的 Cookie，相互不可调用。但部分企业在用户不知情的情况下，通过跨站加代码的方式收集用户在其他网站存储的 Cookie，掌握用户的 Cookie ID、计算机物理地址、浏览记录甚至行动轨迹，将此作为企业的“无形资产”，这种行为显然是不可取的。

二、法律分析

我国的个人信息保护立法正处于不断完善中。2012 年 12 月 28 日，全国人民代表大会常务委员会通过《关于加强网络信息保护的决定》（以下简称《决定》），对“公民个人电子信息”作了界定，并明确了信

息收集、使用的原则和相关规则，明确要求：“网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不得违反法律、法规的规定和双方的约定收集、使用信息。”2013年2月1日，工业和信息化部《信息安全技术 公共及商用服务信息系统个人信息保护指南》（以下简称《指南》）实施，该指导性标准将个人信息分为个人一般信息和个人敏感信息，并提出了默许同意和明示同意的概念；同时，《指南》还提出了处理个人信息时应当遵循的八项基本原则，即目的明确、最少够用、公开告知、个人同意、质量保证、安全保障、诚信履行和责任明确。2013年9月1日，工业和信息化部《电信和互联网用户个人信息保护规定》（以下简称《规定》）开始实施，考虑到信息保护工作涉及众多的部门，工业和信息化部并不负责管理所有的个人信息，为此，《规定》依据《决定》的有关规定，立足工业和信息化部电信和互联网行业管理职责，以“概括加列举”的方式规定了工业和信息化部所负责监督管理的用户个人信息的范围，规定了个人信息收集和使用原则及规则等几项内容。由此可见，在贯彻执行《决定》有关个人信息的收集、使用的制度上，互联网领域已有较成体系的立法，相关行为亦有法可依。我们也可再回头来“溯及既往”地分析“3·15晚会”所反映的问题。

首先，互联网企业可正当利用 Cookie 收集、使用用户信息。如前所述，Cookie 是中立的技术工具，甚至是当前技术环境下必不可少的网络技术，如果妖魔化 Cookie、禁用 Cookie，可能会给用户、企业带来极大不便。而只要互联网企业按照《决定》、《规定》的要求，遵循合法、正当、必要的原则，并经被收集者同意，且采取措施保护个人信息，则利用 Cookie 收集、使用个人信息的行为属合法行为，不存在“泄露隐私”的问题。这里也顺带说明，“个人信息”与“隐私”并非直接对应，二者是不同的法律范畴，用户自行公开的信息不再是“隐私”，但仍可能属于“个人信息”；同时，最高人民法院也正在尝试

以制定司法解释的方式，对涉及个人隐私的司法实践问题的解决进行探索、总结。

其次，如果企业未经用户同意而擅自收集用户个人信息，则会触犯工业和信息化部《规定》。Cookie 中可能包含用户个人信息，利用 Cookie 收集个人信息的行为应受到《规定》约束。而收集用户个人信息应经用户同意。如果在收集用户 Cookie 信息的过程中，没有明确征求用户的同意，告知用户收集信息的目的，则触犯了《规定》。

此外，电信用户经营者与互联网信息服务提供者不得出售或向他人提供用户个人信息。《规定》第十条明确指出，电信业务经营者、互联网信息服务提供者及其工作人员对在提供服务过程中收集、使用的用户个人信息应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。若通过出售包含用户个人信息的 Cookie 数据获取利益，则明显触犯了《规定》。

三、国外立法与借鉴

相较而言，我国的个人信息保护立法还面临着以下问题：互联网产业的发展需要哪些数据？现有立法规定是否完善？如何在确保数据流动以便于行业发展与保护个人信息之间取得平衡？个人信息与隐私有何关系，如何保护个人隐私？这些问题都值得深入研究和探讨，以求完善解决思路，为完善立法、处理保护个人信息与促进产业发展间的关系提供参考。为此，可以参考美国关于权衡互联网发展与个人信息保护的立法。

整体地看，欧美立法力求在个人信息保护与产业发展间寻求平衡。欧盟于 1995 年制定了《关于涉及个人数据处理的个人保护以及此类数据自由流动的指令（95/46/EC）》，并制定了关于向境外转移个人数据的决定（Commission Decision on Standard Contractual Clauses for The Transfer of Personal Data to Third Countries, under Directive 95/46/EC,

2001），为境外主体获得欧盟境内的个人数据提供了可能；美国与欧盟签订了个人信息跨国流通“安全港”协议，都尝试在“保护个人信息”与“促进产业的健康发展”间取得合理平衡。

针对美国互联网企业在欧盟和瑞士境内收集、使用个人信息的行为，美国商务部分别与欧盟、瑞士签订了关于个人信息的“安全港”框架协议，互联网企业的关于个人信息收集和使用的用户隐私政策需满足此框架要求，方可从欧盟境内收集和使用数据。由于欧盟对个人信息的保护采取了较为严格的措施，美国企业若对个人信息保护达不到足够的程度，则不能从欧洲获得用户数据。“安全港”框架协议的要求包括：①告知：服务者应向用户告知“以什么方式，在什么时候，收集什么信息，用途是什么”。②选择性：用户可对个人信息的收集、保存、转移、修改和删除进行自由选择。当然，某些服务的使用，需以提供特定个人信息为前提。③可接触性：应具备必要的途径，保证用户接触其个人信息，进而进行个人信息的修改、删除和更新。④安全性：企业应采取必要的措施，维持数据的安全性，避免数据的遗失、滥用，以及未经授权的接触、泄露、变更和销毁。⑤恰当性：企业应保证所收集的信息适合于相应的利用目的，保证信息的准确性、完整性和“最新性”。⑥向适格者转移：个人信息数据持有者与第三方进行数据转移时，应保证对方也是“安全港”框架内的企业，或对方采取其他方法对用户个人信息提供了应有的保护。⑦实施（可制裁性）：有可供用户进行救济的可行机制；有可供验证该加盟企业是否实施了“安全港”框架要求的程序；有可供补救因未能实施“安全港”框架要求而发生事故的损失的责任。

为方便操作，美国商务部鼓励企业参与行业自律，通过行业认证等制度来确保企业达到“安全港”的最低标准。在该模式下有众多隐私（个人信息）保护认证机构，TRUSTe Privacy Program 作为其中的典型代表，也是世界上最大的“隐私密封方案”，目的在于引导企业采

取措施确保在线安全,同时,TRUSTe 也为消费者提供隐私保护指南。该认证模式通过严格的数据管理要求和用户投诉机制构建起内外结合(企业和用户,还有整个系统)的责任机制,详细要求包括信息收集问题、隐私声明、数据管理等。其核心原则包括透明性、选择性和责任性等:透明性要求所有成员应提供必要的途径,向用户就其隐私政策和实施情况进行告知;选择性要求成员采取措施供用户就成员的信息收集、在线广告服务推送等进行选择;责任性则要求确保用户能就相关问题进行投诉、反馈,同时,成员应承担必要的法律责任。

当然,美国的互联网企业也可直接通过隐私政策的实施来满足“安全港”的最低要求。由于社交网站(以 Facebook 为例)更多地涉及了用户的个人身份信息,因此它们的隐私政策更受关注并饱受指责,为此,社交网站的隐私政策的完善一直是互联网行业持续不断的关注点。当然,这种完善主要体现在隐私政策形式上,包括:措辞更为口语化、更易懂,且以大量的举例来帮助用户理解;采取越来越多的技术措施,供用户在注册、发布信息、与他人交往时,对个人信息的公开、保存和转移进行选择(是否公开或仅好友可见)。而其实质内容与“安全港”框架的要求和类似 TRUSTe 认证的要求并无多大变化。

具体而言,关于 Cookie 的问题,欧洲和美国持不同的立法思路。

欧盟立法明确用户对于 Cookie 的同意原则。2012 年 5 月 6 日,欧盟数据保护新规定出炉,要求使用行为跟踪 Cookies 的网站和广告网络告知他们的用户,更关键的是要征求用户的同意后才能够监测他们的行为数据(当然,这里的“行为数据”应予以区分,对“个人信息”与“非个人信息”区别对待)。

欧盟数据保护工作小组负责制定 Cookie 技术的使用规范,包括在线行为广告、许可和例外等。他们对于 Cookie 指令的意见主要包括以下四条。

（一）“事先知情同意”（Prior Informed Consent）是关键

工作小组认为，用户有权在使用电脑或其他设备之前，获知其是否被“跟踪”。现有的 Cookie 指令中认为“暗示的或推定的同意”（“Implied” or “Implicit” Consent）不足以满足 Cookie 指令要求。

（二）1995 年的数据保护指令仍然可以适用

工作小组认为，1995 年的数据保护指令下的被访问或收集的个人资料、额外的合规性要求仍将适用。1995 年的指令整合了一些重要的数据保护的原则，如数据保存、数据安全、用途限制以及收集敏感数据的义务等。

（三）浏览器许可（Browser Consent）

工作小组还为浏览器许可确立了三个关键要求，达到在 Cookie 指令下提供知情同意的目的：首先，浏览器必须在默认情况下拒绝所有第三方 Cookie（目前市场上并没有这样的浏览器）；其次，浏览器必须参与“许可行动”（Affirmative Action），以接受 Cookie 的设置和传输数据；再次，浏览器必须传达收集到的清晰、全面和完全可见的数据信息。

（四）广告商和发行商的职责

工作小组基于实体是否是一个在线发布者（网站）或广告商，提出了具体的要求。一般而言，工作组根据欧盟法律，审查参与数据控制、目标广告的广告网络和出版商。并且，工作组对于不同的广告网络和出版商，强调了各自不同的责任。

但是，Cookie 指令的具体执行仍存在很多障碍。法国的 CNIL 是目前欧洲为数不多的对数据保护有执法权利的欧盟数据保护机构，但

并没有对任何一家公司执行过处罚（法国的法律规定每一次违规罚款 30 万欧元），并且在实践中很多网站通常利用“使用条款”来规避欧盟的规定；目前强制执行 Cookie 法律的主要联盟成员国是英国，但是英国监管机构 ICO 的执法力度明显不足（他们目前采取的方式是对不符合英国 Cookie 法的网站发警告信）；像意大利和西班牙这样的国家，虽然倾向于对违反数据保护的行为制定严厉的规范，在各自国内 Cookie 法律中要求企业对用户进行“明示许可”，但在法律的具体执行上，也总持沉默态度。

美国则注重行业自律，发起“Do not Track”计划。目前，美国对于 Cookie 的隐私问题的解决方式主要依赖于技术进步和市场自律，而不是强制的法律规制，其中最主要的行动是 Do not Track。

2010 年 12 月，FTC 发布的隐私报告中要求设计一个“Do not Track”系统，让用户能控制自己在网络上的隐私信息。一周后，微软宣布其下一款浏览器（IE9）将会提供一个阻止第三方追踪的黑名单，以保护用户的隐私不被追踪。

当用户提出“Do not Track”请求时，具有“Do not Track”功能的浏览器在 http 数据传输中添加一个“头信息”（Headers），这个“头信息”向商业网站的服务器表明用户不希望被追踪，这样，遵守该规则的网站就不会追踪用户的个人信息来用于更精准的在线广告。

值得注意的一点是，Do not Track 功能类似于 Robots Exclusion 标准，提供一种机制使客户端自动在 http 服务中发送一个请求给服务端，但是完全依赖于服务端的是否自律，也就是说广告商可以忽略这个机制。有些公司同意不再将用户数据用于保险、医疗等行业，但是依然有可能会用在市场研究和产品开发中，比如 Facebook 主页上的“追踪”按钮并不会被阻止。

如前所述，欧盟和美国对于 Cookies 的立法管理模式有较大的区别。

欧盟在最早制定个人数据保护立法时就崇尚对个人信息自决权的保护，在个人权利的保护与互联网发展创新这两个矛盾中，欧盟立法更倾向于对个人权利的保护，该立法指导思想一直延续至今。美国对于互联网的管理一直崇尚的是保护创新，倡导行业自律，不通过严格的法律来限制企业的行为，因此美国个人信息保护在个人权利保护与发展创新之间，选择了后者。美国的这种保护模式，在促进企业发展与创新方面确实起到了积极作用，目前全球排名靠前的互联网企业几乎都来自美国，而在欧洲却缺少这种大型的互联网企业。欧盟关于个人信息保护的严格立法在某种程度上也是对美国互联网巨头企业的一种制衡。

由此可见，欧盟与美国处理 Cookie 隐私问题的区别主要包括两个方面，首先在于理念：欧盟倡导严法治理，美国倡导行业自律。这与欧洲一直以来强调个人信息的保护有关；而美国更看重互联网行业的创新与发展，希望给用户提供更贴心和顺畅的服务。其次，操作方式上也存在不同：通过对欧盟《Cookie 指令》的分析可以看出，欧盟要求用户给予网站“明示许可”，即网站在用户接入前就要征得许可，并且向用户提供所收集 Cookie 的目的，属于 opt-in 机制，最大限度地保护用户的知情与选择权；而美国所采用的“Do not Track”机制则是在互联网服务提供商和用户之间进行了平衡，用户可以选择不让网站跟踪自己的登录、浏览行为，但如果不采取设置或行动，则属于默示许可，即 opt-out，但用户可以在任何时候选择退出跟踪。目前多数的主流浏览器都采用了这种方式，并且 FTC 的有关隐私报告对这一模式予以了肯定。

四、总结和评述

可考虑参考美、欧关于个人信息保护与数据流动的立法经验，继续完善我国的个人信息保护立法。《电信和互联网用户个人信息保护规定》在《全国人民代表大会常务委员会关于加强网络信息保护的決定》之后，

对电信和互联网用户个人信息保护进行了具体规定，它以界定“何谓‘个人信息’”为基础，对个人信息的收集、使用等作了科学、合理的规定，但对促进数据流动与互联网行业发展的问題没有直接作出回应。

就 Cookie 的具体问题来看，需要先对 Cookie 本身进行界定。考虑到并不是所有的 Cookie 都是个人信息，不能笼统地要求所有关于 Cookie 的行为都遵守《决定》和《规定》的要求，只有涉及“个人信息”的，才适用前述法律条文的规定。

此外，互联网行业对于 Cookie 数据的应用存在一定的依赖性。如通过收集用户购物习惯，向用户推送商家优惠信息，或者通过数据的分析处理，给用户推荐更贴近用户习惯的服务等，都为的是向用户提供更好的服务。因此，对 Cookie 而言，采取欧盟那种“一刀切”的方式显然是不现实的，不仅会降低用户使用网络的流畅性，还会对网络广告行业造成很大的损失，而应该回到《关于涉及个人数据处理的个人保护以及此类数据自由流动的指令》所规定的“促进数据自由流动”，在个人信息保护与行业发展间取得平衡，使 Cookie 同时也能满足行业发展所需。美国采取的“Do not Track”机制更依赖行业的自律，通过行业协会的力量来实现对用户 Cookie 信息的安全使用。通过“3·15晚会”曝光此类地下利益链条片面地揭示了 Cookie 的问题，没有全面地看到中立的 Cookie 技术的积极作用，但也促使我们思考如何更好地规制个人信息的收集、使用的行为。

综上所述，在区别对待“个人信息”与普通的“数据”，对涉及个人信息的行为适用严格标准的前提下，可以考虑通过立法，为行业所必需的用户数据使用行为提供合理空间。在涉及 Cookie 的具体问题上，可以综合欧美两种不同的立法模式，根据我国国情，建议通过以下几种方式对不法使用 Cookie 的行为进行规范。

(1) 可通过第三方机构对不同网站进行安全评级，若安全等级较低，则需要向用户提供“明示许可”，经用户确认后才可收集用户

的 Cookie 信息；对于安全等级比较高的网站，可设置为“默认许可”，但是浏览器应包含“Do not Track”按钮，用户可选择是否被网站跟踪。

（2）网站向用户获取许可时，应以简单、明确、易懂的方式告知用户 Cookie 信息收集的用途及收集方式，是否被第三方网站使用等。

（3）倡导网络广告行业自律，在行业内形成良好的氛围，由工业和信息化部相关部门对企业进行定期查验，确认其是否违反《电信和互联网用户个人信息保护规定》。

第十四章 互联网市场竞争频现里程碑式案件

一、概述

（一）腾讯诉奇虎不正当竞争纠纷案

2006年12月，腾讯进军网络安全领域，其推出的QQ医生1.0beta版就是用于防止盗号查杀木马。2009年，腾讯推出QQ医生3.2版，该版本从界面到功能都与奇虎360安全卫士相类似。2010年春节，腾讯在二、三线及以下城市积极推广QQ医生。

2010年9月，奇虎360方面推出由奇智软件有限公司发行的“360隐私保护器”。在发布隐私保护器的同时，奇虎360安全中心官方网页上刊文称，近期接到大量用户投诉，称某聊天软件在未经用户许可的情况下偷窥用户个人隐私文件和数据。随后，360公司谴责称“这种窥视用户隐私的行为与流氓软件的行为完全一致”，严重损害了用户的利益。

2010年9月27日，腾讯首次发表声明，称该隐私保护器是对腾讯QQ安全功能的误解，“将QQ安全检查模块的例行安全检查和QQ用户的正常操作列为‘QQ窥视用户隐私’行为”。10月11日，腾讯QQ产品团队再次发布“关于腾讯QQ被诬蔑‘窥视用户隐私’的严正声明”。该声明详细解说QQ安全检查原理和机制，并提出“360有故意抹黑行为”，同时宣布“采取法律途径维护正当权益”^①。

^① 具体参见北京市朝阳区人民法院民事判决书（2010）朝民初字第37626号。

2010年10月14日，腾讯科技公司、腾讯计算机公司向北京市朝阳区人民法院提起诉讼，要求北京奇虎科技有限公司（“360隐私保护器”的开发者和著作权人、“360网”的域名注册人，以下简称“奇虎科技有限公司”），奇智软件有限公司（“360隐私保护器”的发行人）和三际无限网络科技有限公司（“360网”的实际经营者，以下简称“三际无限公司”）停止侵权、公开道歉并作出赔偿。

2011年4月26日，北京市朝阳区法院就腾讯起诉奇虎360不正当竞争案作出一审判决，奇虎科技有限公司等三个被告停止发行使用360隐私保护器，连续30日公开发表声明，消除因侵权行为对腾讯造成的不利影响，赔偿40万元，并在360网站上删除相关侵权言论。

一审宣判后，三际无限公司、奇虎科技有限公司不服判决，向北京市第二中级人民法院提起上诉。经过审理，北京市第二中级人民法院认为上诉人奇虎科技有限公司和上诉人三际无限公司的上诉理由均不能成立，其上诉请求，均不予支持。原审判决认定事实基本清楚，适用法律正确，应予维持。2011年9月14日，北京市第二中级人民法院作出终审判决：驳回上诉，维持原判。

2011年6月10日，腾讯公司、腾讯计算机公司向广东高级人民法院起诉奇虎科技有限公司、奇智软件有限公司“扣扣保镖”不正当竞争纠纷。广东省高级人民法院一审判决，奇虎科技有限公司、奇智软件有限公司构成不正当竞争，连带赔偿腾讯公司、腾讯计算机公司经济损失及合理维权费用共计500万元。奇虎科技有限公司、奇智软件有限公司不服一审判决，2014年2月28日，最高人民法院终审判决维持广东高级人民法院的一审判决，认为360扣扣保镖软件违背了诚实信用原则和公平竞争原则，对QQ软件构成不正当竞争，360被判向腾讯赔礼道歉、消除影响，并赔偿人民币500万元。

（二）百度诉奇虎 360 侵犯商标权及不正当竞争（插标行为与劫持流量行为）

2012 年 3 月，百度公司针对奇虎 360 向北京市第一中级人民法院提起诉讼。百度称，360 通过安全卫士 beta 版，在百度搜索时默认开启插入标签功能，未经百度允许强行对百度搜索结果进行标注，篡改百度搜索结果页面，混淆和误导了普通用户。当用户点击该搜索结果后会弹出 360 网盾提示页面，通过提示用户“我要安全上网”，向用户宣传并误导用户安装其浏览器，为其 360 浏览器导流，造成不正当竞争。

百度公司认为，奇虎 360 利用 360 浏览器捆绑其网址导航站，故意仿冒、混淆百度搜索结果，劫持百度流量，侵犯原告商标权并且不正当竞争。

奇虎 360 方面称，其“标注拦截虚假医药等恶意网站”、“保障网民安全上网”，是为保障网民用户的利益，并不涉及不正当竞争。

北京市第一中级人民法院判决如下：一、被告北京奇虎科技有限公司自本判决生效之日起立即停止涉案的不正当竞争行为；二、被告北京奇虎科技有限公司在本判决生效之日起七日内，连续十五日在网站 www.360.cn 首页显著位置刊载消除影响的声明（该声明应当事先由本院审核通过，如被告北京奇虎科技有限公司拒绝执行，本院将在《人民法院报》上刊登本案判决书相关部分，所需费用由被告北京奇虎科技有限公司承担）；三、被告北京奇虎科技有限公司自本判决生效之日起七日内赔偿原告北京百度网讯科技有限公司、百度在线网络技术（北京）有限公司经济损失四十万元；四、被告北京奇虎科技有限公司自本判决生效之日起七日内赔偿原告北京百度网讯科技有限公司、百度在线网络技术（北京）有限公司合理支出五万元；五、驳回原告北京百度网讯科技有限公司、百度在线网络技术（北京）有限公司的其他诉讼请求。

一审宣判后,奇虎科技有限公司不服判决,向北京市高级人民法院进行上诉。8月13日上午,百度诉奇虎360侵犯商标权及不正当竞争案在北京市高院二审开庭,因上诉方向法院提交多项新证据,被上诉人因此要求延期质证,该案未当庭宣判。

二审中,百度和360双方还针对360安全软件是否篡改源代码、360网址导航站中设置的下拉提示词是否对百度造成影响等多个细节问题展开了激烈的法庭辩论。奇虎科技有限公司在法庭规定的时间内向法庭提交了5份新证据,符合司法程序以及相关规定。法院要求百度对这5份新证据在3~5个工作日内提出质证意见并决定择日开庭作出终审判决。

(三) 百度诉奇虎360违反 Robots 协议不正当竞争

2012年8月15日,奇虎360低调推出综合搜索。短短几天即超越搜狗、搜搜和Google,成为仅次于百度的中国第二大搜索引擎。8月27日,百度与奇虎360搜索正面交锋,百度将奇虎360综合搜索中百度知道、百科、贴吧等产品进行搜索屏蔽,用户使用奇虎360综合搜索将被强制跳转到百度首页,“3百大战”爆发。奇虎360随后展开反攻,使用奇虎360搜索点击百度相关服务的用户直接被带至“网页快照”页面。

2013年1月26日起,不少百度推广系统的商家在使用奇虎360浏览器登录百度管理后台时,被百度要求必须安装一个安全插件,该插件禁止用户使用奇虎360浏览器登录,并建议使用IE、火狐、谷歌或者百度浏览器登录后台。

1月28日,奇虎360紧急召开发布会,相关负责人指出,百度正在大规模部署“偷拍插件”。它在未作任何提示、未经用户允许的情况下,暗中对用户电脑屏幕截图,并把图片上传到百度服务器。

360指出,一旦用户电脑安装该插件,百度便能够判断出用户正

在使用哪款浏览器上网，再专门针对 360 浏览器进行不兼容提示。该插件会采集用户系统信息，包括 CPU 信息、磁盘序列号、网络地址和网卡信息、当前所有进程列表和浏览器进程名，并在用户登录百度“凤巢推广系统”^①时对电脑屏幕截图，再将这些信息一并上传到百度服务器，以此识别和封杀 360 浏览器，甚至利用这些信息向用户推送“精准广告”。

百度诉奇虎 360 违反“Robots 协议”抓取、复制其网站内容侵权一案，2013 年 10 月 16 日上午在北京市第一中级人民法院开庭审理。

（四）360 诉腾讯公司滥用市场支配地位纠纷案

2010 年 11 月 3 日，腾讯在致所有 QQ 用户的公开信中宣称，公司将在装有 360 软件的电脑上停止运行 QQ 软件，并提醒用户只有卸载 360 软件才可登录 QQ，此举引发广泛反响。事后据统计被迫卸载的 360 软件的用户达到近 6000 万。2011 年奇虎向广东省高院起诉腾讯科技（深圳）有限公司和深圳市腾讯计算机系统有限公司，主张两被告借助即时通信服务搭售网络安全软件的行为和“3Q 大战”期间的“二选一”做法均属违反《反垄断法》的滥用市场支配地位行为。

广东省高院驳回原告北京奇虎科技有限公司的全部诉讼请求。认为由于互联网行业特殊的市场状况，尤其不能将市场份额作为认定经营者市场支配地位的决定性因素。即使在原告所主张的最窄的相关市场内，正如 CNNIC 报告所述，腾讯的市场优势地位并未抑制和缩小其他即时通信产品的市场发展空间，亦不构成该市场整体发展的阻碍因素。腾讯在该市场不具有支配地位。原告所诉被告实施了滥用市场支配地位的搭售行为不能成立。

① “凤巢”是全新的百度搜索推广服务管理平台的内部开发代号。通过这一全新平台，客户可以对百度搜索推广信息进行更为高效的管理与优化，对推广效果更为科学地进行评估。

奇虎 360 不服广东省高院判决结果，随即向最高人民法院提出上诉，最高院决定于 11 月 26 日对此案进行公开开庭审理。奇虎 360 二审的诉讼主张是，请求法院判令腾讯停止涉案滥用市场支配地位的行为，要求腾讯赔偿经济损失 1.5 亿元，并公开赔礼道歉。2013 年 11 月 26 日上午 9 时，最高人民法院第一法庭公开开庭审理上诉人北京奇虎科技有限公司与被上诉人腾讯科技（深圳）有限公司、深圳市腾讯计算机系统有限公司滥用市场支配地位纠纷一案。目前本案尚未作出判决。

二、法律分析

（一）3Q 不正当竞争案中“360 隐私保护器”的监测行为是否属于不正当竞争

奇虎科技有限公司、奇智软件有限公司认为“360 隐私保护器”与 QQ 软件两款软件在功能作用、目标用户上都不相同，两者不构成竞争关系。“360 隐私保护器”是一个中立的软件，它只是对 QQ 软件等产品进行监测并将其在用户计算机后台运行的情况如实记录下来，将这些软件扫描或查看已安装软件和文件信息的情况报告给用户，对可能涉及用户隐私的状况作出提示。“360 隐私保护器”只是提示“被 QQ 查看过的文件，有可能涉及您的隐私”。监测结果只是对软件行为的如实记录，反映的是客观事实，并没有捏造事实，更不是诋毁商誉，因此不构成不正当竞争。

法院认为，从涉案产品的用户群看，在本案中，“360 隐私保护器”只针对 QQ 软件进行监测，具有唯一针对性，因此“360 隐私保护器”是依附于 QQ 软件运行，从而“360 隐私保护器”的用户群也是 QQ 软件的用户群。由于双方的客户群是同一个，从而使得两产品的经营者之间形成竞争关系。从上述两点看出，无论是从经营范围，还是涉案产品的用户群上，双方之间存在竞争关系。

就竞争行为方面，奇虎科技有限公司、奇智软件有限公司和三际无限公司对“360 隐私保护器”开发、发行以及对 QQ 软件的评价行为，会产生对“360 隐私保护器”经营者增加自己的竞争优势或降低腾讯科技公司、腾讯计算机公司竞争优势的后果，属于竞争行为。

（二）3Q 不正当竞争案中的 360 扣扣保镖是否构成不正当竞争

腾讯观点：“360 扣扣保镖”自称有给 QQ 体检、帮 QQ 加速、清理 QQ 垃圾等功能，“实质是打着保护用户利益的旗号，污蔑、破坏和篡改腾讯 QQ 软件的功能，同时通过虚假宣传，鼓励和诱导用户删除 QQ 软件中的增值业务插件、屏蔽原告的客户广告，同时将其产品和服务嵌入原告的 QQ 软件界面，借机宣传和推广自己的产品”。

360 观点：扣扣保镖是个创新型工具软件，不涉及 QQ 核心聊天功能，不会触碰用户的 QQ 账号密码和聊天记录等；相反，扣扣保镖会大幅度提高 QQ 账号、密码、聊天记录的安全等级，扣扣保镖所有的行为都是用户主动点击触发的，提升用户在使用该软件时的体验，扣扣保镖充分尊重了用户的选择权。

一审法院认为：

第一，关于被告扣扣保镖是否能够破坏原告 QQ 软件及其服务的安全性、完整性，使原告丧失增值业务的交易机会及广告收入，从而构成不正当竞争的问题。

被告针对原告 QQ 软件专门开发的扣扣保镖破坏了原告合法运行的 QQ 软件及其服务的安全性、完整性，使原告丧失合法增值业务的交易机会及广告、游戏等收入，偏离了安全软件的技术目的和经营目的，主观上具有恶意，构成不正当竞争。

第二，关于被告在经营扣扣保镖软件及其服务时，是否存在捏造、散布虚伪事实，从而构成商业诋毁的问题。

被告针对原告的经营，故意捏造、散布虚伪事实，损害后者的商业信誉和商品声誉，构成商业诋毁。

第三，关于被告的扣扣保镖是否通过篡改 QQ 的功能界面从而取代原告 QQ 软件的部分功能以推销自己的产品，构成不正当竞争的问题。

被告以保护用户利益为名，推出扣扣保镖软件，诋毁原告 QQ 软件的性能，鼓励和诱导用户删除 QQ 软件中的增值业务插件、屏蔽原告的客户广告，其主要目的是将自己的产品和服务嵌入原告的 QQ 软件界面，依附 QQ 庞大的用户资源推销自己的产品，拓展 360 软件及服务的用户。被告在给原告造成了严重经济损失的同时推销自己的产品，增加自己的交易机会，违反了诚实信用和公平竞争原则，构成不正当竞争。

第四，技术创新、自由竞争和不正当竞争的界限，扣扣保镖是否跨过了技术创新与不正当竞争的界线问题。

最高法院认为，互联网的发展有赖于自由竞争和科技创新，互联网行业鼓励自由竞争和创新，但这并不等于互联网领域是一个可以为所欲为的法外空间。是否属于互联网精神鼓励的自由竞争和创新，仍然需要以是否有利于建立平等公平的竞争秩序、是否符合消费者的一般利益和社会公共利益为标准来进行判断，而不是仅有某些技术上的进步即应认为属于自由竞争和创新。360 以技术创新为名，专门开发扣扣保镖对被上诉人 QQ 软件进行深度干预，难以认定其行为符合互联网自由和创新之精神。

（三）3B 不正当竞争案中的 Robots 协议是否具有法律效力

搜索引擎 Robots 协议，也称为“爬虫协议”、“机器人协议”、“蜘蛛协议”。这个协议对搜索引擎抓取网站内容范围作了约定，包括网站是否希望被搜索引擎抓取，哪些内容不允许被抓取，于是“网络爬

虫”依据协议的内容“自觉地”抓取或不抓取这个网页的内容。百度的 Robots 协议不允许 360 抓取，而 360 抓取了，是否构成不正当竞争。

百度方面称，在百度对百度网站设置了明确的权利声明和技术措施的情况下，360 公司违反“Robots 协议”、百度权利声明和技术措施，抓取百度网站页面并生成“快照”复制件存储于被告自身服务器中，构成不正当竞争，侵犯了百度合法权益，给其造成巨大损失。

360 方面则称，这些内容页面实际上是由网友提供的，根据互联网的通行规则，这些页面的版权属于网友，360 搜索索引这些内容页面并不侵犯百度的知识产权。360 认为百度自创了专门针对其的白名单机制，是歧视性条款。

360 认为，百度以 360 违反 Robots 协议起诉 360 公司，是滥用 Robots 协议打压竞争对手。百度与 360 之争，并不是两家搜索引擎之间的竞争，而是百度将百度知道、百度贴吧、百度文库等由网友创作的内容页的相关权益据为己有，同时设定歧视性条款，单独拒绝 360 搜索来索引。

360 还称，百度以附加白名单的方式滥用 Robots 协议，目的是保住其在搜索市场的垄断地位，利用技术手段设置壁垒，打击 360 搜索作为中国第二大搜索引擎的有序竞争，实质是百度的不正当竞争行为严重破坏了互联网市场互联互通和信息共享等基本原则。

（四）3Q 垄断案中的相关产品市场如何界定

奇虎公司提出：QQ 即时通信软件及相关服务市场，根据其独特的定价以及盈利模式，难以被其他通信服务替代，应构成独立的商品市场。该市场因其独特的中文语言、文化背景，地域间不存在替代关系，应界定为中国境内市场。

腾讯公司回应：原告界定市场错误。除 QQ 外，市面上还有

MSN、微博、电子邮箱、米聊等各式各样的即时通信服务；即时通信服务本身只是通信服务的一种，其与短信、手机、电话等传统通信产品，电子邮箱、微博、SNS 等社交网络间存在需求替代关系。由于互联网的开放性和互通性，即时通信的用户并不局限于中国大陆。腾讯公司还指出，现在的互联网竞争是平台竞争，正如 MSN 整合游戏、邮箱、搜索等服务，新浪微博用微博吸引大量用户，又通过广告、微音乐、微桌面等整合平台，提供多种服务，许多互联网企业都是通过搭建平台，支撑它的免费服务。通信服务市场是不存在的，实际上是平台市场的竞争。

广东省高院对奇虎诉腾讯滥用市场支配地位行为案作出了判决，该案使用了假定垄断者测试法（SNNIP）来界定腾讯免费即时通信软件是否与其他免费互联网服务属于同一个相关产品市场。法院确定本案相关商品市场的界定可以采取下列方法：根据需求者对 QQ 软件及其服务的功能用途需求、质量的认可、价格的接受以及获取的难易程度等因素，从需求者的角度定性分析不同商品之间的替代程度；同时亦结合考虑供给替代的影响。法院认为原告关于综合性的即时通信产品及服务构成一个独立的相关商品市场的主张不能成立，法院不予支持。

（五）3Q 垄断案中腾讯公司在相关市场上是否具有支配地位

奇虎公司表示，根据艾瑞咨询公司提供的数据，QQ 的市场份额达 76.2%；中国互联网中心出具的调研报告也显示，QQ 软件的渗透率为 97%。腾讯 2010 年财报显示，其全年收入高达 196 亿元，盈利能力远超同类企业。从技术条件来看，腾讯在即时通信方面的专利保有量占全国的 80% 以上。

360 在 3Q 垄断案中聘请的专家辅助人 David Stallibrass 在欧洲独立提供竞争法调查经济意见机构 RBB 的报告中称，QQ 过去 5 年的即时通信市场份额为 70%，中国电信的即时通信服务飞信的市场份额不超

过4%，2010年，QQ的市场份额是飞信的33倍。

腾讯公司认为，艾瑞公司对市场份额定义在时间、销售数量等标准和反垄断法的规定存在较大差异，证明力不足，且渗透率是市场份额。一个用户可开多个QQ账户，市场用户多不等于市场份额。腾讯没有市场定价权。

法院认为，奇虎360以并不具备真实基础的市场份额来推定被告在相关市场上具有垄断地位的主张本院不予认可。因为腾讯不具有控制商品价格、数量或其他交易条件的能力，不具备阻碍、影响其他经营者进入相关市场的能力。由于互联网行业特殊的市场状况，尤其不能将市场份额作为认定经营者市场支配地位的决定性因素。即使在原告所主张的最窄的相关市场内，正如CNNIC报告所述，腾讯的市场优势地位并未抑制和缩小其他即时通信产品的市场发展空间，亦不构成该市场整体发展的阻碍因素。腾讯在该市场不具有支配地位。

三、国外立法与借鉴

（一）关于不正当竞争

第一，关于竞争关系的认定。

（1）世界知识产权组织的《反不正当竞争示范条款》认为，“在工商业活动中违反诚实信用的任何行为都构成不正当竞争行为”，该条款的注释中特别强调，反不正当竞争法同样适用于当事人之间没有直接竞争关系的情况。这就是说即使当事人实施的行为没有指向竞争对手，但只要当事人的行为降低了他人的竞争能力，就说明存在竞争关系。

（2）《保护工业产权巴黎公约》（以下简称《巴黎公约》）对不正当竞争行为作出了概括，《巴黎公约》第10条之2第2款规定：“凡

在商业活动中违背诚实惯例的竞争行为，即构成不正当竞争。”

第二，关于商业诋毁。

（1）德国 1998 年修订的《反不正当竞争法》，将商业诋毁描述为恶意编造或传播针对其他经营者的商品、营业业务、企业主或领导人的虚假事实，足以对其他经营者造成损害的行为。

（2）日本的《不正当竞争防止法》规定商业诋毁为以侵害他人在经营业务上的信誉为目的，陈述、散布虚假信息的行为。

（3）《巴黎公约》将商业诋毁规定为在工商业活动中诋毁竞争对手的营业所、商品或经营活动的行为。

（4）世界知识产权组织的《反不正当竞争示范条款》将商业诋毁的行为分为两类：一类是以“虚假”说法为行为内容，即凭空捏造、散布有关其他经营者商誉的，与其他经营者商业信誉、商品声誉的真实情况不吻合的事项，包括完全属于无中生有的凭空编造，也包括对一定事实真相的恶意歪曲。另一类是以“不当”说法为特征的行为，即陈述客观事实时有意不公正、不准确、不全面地进行描述，其目的在于在贬低或者诋毁其他经营者的商誉。

（二）相关市场界定

美国 1992 年《司法部和联邦贸易委员会横向合并指南》（以下简称 1992 年《横向合并指南》）认为，“市场可以定义为一种产品或一组产品及生产和销售这种（些）产品的一个地理区域，对这种（些）产品和这个地理区域来说，在假设所有其他产品的销售条件不变的情况下，如果这个市场上现在和未来只存在唯一的厂商，而且假定该厂商的定价不受管制并以追求利润最大化为目标，那么这个厂商很可能会采取‘小而显著非短期’（Small but Significant and Non-transitory）的提价方法获利”。

1989年12月21日的《欧共体部长理事会关于控制企业之间合并行为的4046/89号法规》（以下简称1989年《合并条例》）第9条第7款规定，“相关地域市场应当包括有关企业从事商品或服务的供求业务的地域范围，该地域的竞争条件足以一致并且由于与相邻地域内的竞争条件存在显著差别，而与相邻地域得以区别。”“在进行此项评价时，应当考虑到有关产品或者服务的性质和特征，市场进入障碍的存在，消费者的喜好、相邻地区的企业之间在市场份额方面的显著差别，以及显著的价格差异等。”但这里仅对地理市场作了规定。

1997年12月9日，欧共体委员会发布的《关于界定欧共体竞争法中相关市场的通告》（以下简称1997《相关市场界定通告》）从产品范围和地域范围两个方面对相关市场进行了界定。该通告第7段指出：“相关产品市场是指根据产品特性、价格及用途，而被消费者视为可互换（Interchangeable）或可相互替代（Substitutable）的所有产品和/或服务。”第8段则指出：“相关地域市场指的是所涉企业进行产品或服务供求活动的地区，该地区的竞争条件是充分同质的（Being Sufficiently Homogeneous），并与相邻地区的竞争条件明显不同，因而能将其与相邻地区区分开来。”欧共体委员会在1998年发布的447/98号条例的附录《有关第4064/89号条例的并购申报之格式（Form CO）》也有关于相关市场的界定。在其判例中，欧洲法院1979年关于Hoffman-La Roche案中，已明确对相关市场的概念表达了自己的主张，即“属于该市场的商品之间存在着有效竞争的可能性，并且以此作为前提，在属于同一市场的所有商品之间存在着具有相当程度的相互交换的可能性。”

1992年美国司法部颁布的里程碑式的《横向兼并指南》中提出了现在普遍使用的相关市场界定SSNIP（假定垄断者标准）方法，该指南发布后，美国法院在审理反垄断案件的相关市场界定中采取了较为一致的做法，改变了以往案例中对相关市场界定随意且过窄的缺陷。

美国联邦贸易委员会 2010 年 8 月 19 日正式发布的 2010 年平行合并指南对市场界定进行了顺应现实的改革，指南不要求对每一起平行合并案件都进行相关市场界定，适度降低了相关市场界定在反垄断案件中的重要性。

（三）市场支配地位认定

德国《反限制竞争法》第 19 条第 2 款对市场支配企业的描述：“作为某一特定类型的商品或服务的供给者或需求者，如果某一企业在相关产品市场和地域市场上符合了以下条件，即具有市场支配地位：①没有其他竞争者或者没有受制于实质性竞争，或者②相对于其他竞争者具有突出的市场地位；在此，尤其（但不限于此地）要考虑它的市场份额、财力、采购渠道或者销售渠道，与其他企业的关联关系，其他企业进入市场所面临的法律上或事实上的障碍，本法适用的地域范围之内或之外的企业与它之间现存的或潜在的竞争，它将自身的供给或者需求转向其他商品或者服务的能力，以及它的交易相对人转而从其他企业获得商品或服务的可能性。”

在认定市场支配地位时，欧盟和德国都很看重企业五类结构性特征：①企业纵向一体化能力，②提供富有差异性的产品或灵活调整供需产品的能力，③上下游交易相对人对被考察企业的依赖性，④企业经济实力，⑤技术条件与创新能力。

四、总结和评述

当前，我国互联网网络 and 用户稳步增长，互联网产业初具规模，互联网继续渗透到经济和社会活动中，力助国民经济发展和加快信息化进程。互联网应用多样化，应用前景广阔。与此同时，互联网市场竞争仍存在一些深层次的问题亟待解决。互联网行业的竞争不仅是互联网企业之间利益的竞争，而且影响到广大互联网用户的切身利益，

更涉及国家知识创新战略，关系到国家综合竞争力的提升。技术日新月异导致互联网企业的支配地位不稳，知识产权、标准、关键性设施日益成为直接约束互联网产业链相关主体的重要因素，这些都使得互联网市场竞争和垄断问题较传统市场竞争和垄断问题更具复杂性，对互联网行业发展和管理带来了巨大挑战。

因此，现阶段应完善竞争执法机构与互联网行业主管部门之间的执法协调和配合机制，进一步发挥行业主管部门的产业引领和创新促进作用。双方应通力合作，联合出台相关规定，竞争执法机构在互联网行业的限制竞争和反垄断案件时应当征求行业主管部门的意见。双方应建立信息交换机制、意见征询协商机制，对于涉及共同管辖事项，双方事前进行必要沟通磋商及意见征询，加强执法阶段的沟通和协调，创造良好的互联网行业竞争秩序，共同推进我国互联网行业竞争秩序的规范化和行业健康发展。

第十五章 “棱镜计划”引发全球关注

一、概述

2013年6月6日，美国华盛顿邮报和英国卫报同时刊出由爱德华·斯诺登爆料的“棱镜计划”（以下简称“棱镜”）。据称，该计划是美国国家安全局实施的绝密级电子监听项目，由时任总统小布什于9·11事件之后启动。棱镜可实时监控个人网络活动，监听信息范围包括10类信息：电子邮件、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间和社交网络资料的细节。通过棱镜，国家安全局可以将个人的网络活动尽收眼底。之后，包括谷歌、雅虎、微软和Facebook在内的多家美国互联网企业被曝遭要求提供用户数据；谷歌率先对美国政府提起诉讼，称依照美国宪法第一修正案，他们应获得披露政府行为细节的权利，以维护因斯诺登“棱镜门”事件而受损的公司名誉；随后，Facebook公布数据称，2012年下半年，总计收到9000~10000次政府信息索求，公司配合了其中的79%，涉及1.8万~1.9万用户账户。

二、法律分析

“监听”是一个诉讼领域的法律术语，是指基于犯罪侦查或保障国家安全目的，由执法机关或情报机关依据法律条文对特定目标（个人或机构）的通信予以拦截、留存并读取的行为。放眼全球，包括美国在内的很多国家都针对监听制定了严格的法律，监听的启动事由、程序、范围、信息留存等方面都有严格的法律控制。时至今日，在这

一高度信息化的时代，国家间的监听监控其实由来已久，各国对此心知肚明，“棱镜”的曝光之所以引起如此大的反响，主要是因为大家都惊讶于美国情报机构的监听范围如此之广，程度如此之深，几乎涵盖了各国各行业的方方面面，可谓全天候无缝监控全球。

从美国国内看，棱镜项目在美国法律中可以找到依据，具体分析如下。

其一，从美国监听法律条文来看，棱镜项目既符合法律实体规定，也符合法律程序。从授权上看，国家安全局执行棱镜项目，要求互联网服务提供商和电话运营商交出信息数据，主要是依据《爱国者法案》第 215 节。例如，国家安全局要求电信运营商 Verizon 公司，要持续向国家安全局提交所有的美国国内和国际电话记录。从操作程序上看，棱镜依据的是《外国情报监视法案 2008 修正案》（FAA 2008）第 702 节，根据该节规定，国家安全局在锁定监控目标之后，要向外国情报监视法庭递交申请，法庭批准之后会发出批准令，国家安全局据此实施监控。

其二，从企业角度看，互联网服务提供商、电话运营商向国家安全局递交信息数据的举动，实为一种“配合”，虽然是在公民（消费者）不知情的情况下，但依据美国法律，企业的“配合”举动，是法律义务，不“配合”就是违法，会受到追究。因此，从某种程度上看，在强大的国家机器面前，即使如谷歌、微软这样的跨国巨头，在配合情报机构执行监听义务方面，也没有过多讨价还价的空间。总体上看，美国主要是通过《通信协助执法法》、《爱国者法案》、《外国情报监视法（修正案）》等多部法律，将电信运营商、互联网企业、网络电话服务提供商等众多类型的电子通信服务企业纳入辅助监听的义务提供者的范围，具体义务包括：配合国家安全局等情报机构完成数据索取要求；修改设备和接口为执法机关预留必要“通道”；监听过程中，启动设备交换机中的监听通道，传输监听对象的通信数据等。因此，在法律条文的规制下，一旦企业违背了法定义务，后果将是十分严重

的。例如，依据《外国情报监视法》第 702 节之规定，企业如果不按照外国情报监视法庭的授权令将相关情报信息提供给前来索取信息数据的情报机构，将面对法庭的强制执行令，被要求强制提交，更有甚者，可以“藐视法庭罪”论处。

其三，棱镜事件考量着信息安全立法者在“安全”和“公民隐私”两个价值砝码上的重量选择。棱镜计划说明，在公民隐私权和国家安全孰轻孰重的问题上，美国监听法律制度的天平已经倾向于后者。这种以牺牲隐私换取安全的做法遭到了美国国内及国际社会的广泛质疑。国内民众认为这是在拿隐私权与所谓的安全议题做交换。棱镜在欧盟社会、政府也激起激烈愤慨，欧盟委员会副主席、司法专员维维亚娜·雷丁（Viviane Reding）致信美国司法部部长霍尔德：“授权实施‘棱镜’所依据的美国法律，给欧盟公民的基本权利带来了严重的负面影响。”雷丁希望美方对欧盟的有关忧虑作出答复，并表示将根据答复来重新评估美、欧之间关于数据共享的“安全港”协议。而事实上，无论外界反应如何，美国自 9·11 事件之后所出台的系列法律已经清楚地表明了态度，在“安全”和“公民隐私”之间选择前者。

三、未来趋势

即便“棱镜”遭到多方指责，但美国依然我行我素，这一趋势可从美国立法机构、行政执法机构的一系列举动中一窥端倪。

2012 年 11 月，棱镜计划被国会批准延展五年，有效期截至 2017 年 11 月。

2013 年 7 月 21 日，美国国家情报总监办公室发布正式公告，称依据美国《爱国者法案》，为棱镜监听项目颁发法庭授权令的美国外国情报监视法庭再次向国家安全局进行了新一轮授权，这意味着棱镜项目再获法律放权。

2013年7月24日,美国众议院投票否决了《国防授权法案(修正案)》中不再为国家安全局的监听行动进行财政拨款的提案,这意味着,棱镜计划的实施机构——国家安全局在下一个财政年度,仍然可以获得专门的财政支持,继续实施全球监控。

2013年9月,美国国会召开棱镜情报系统改革听证会,这是棱镜事发3个月之后,美国立法机构首次正式的实质性回应。听证会围绕《情报控制和监控改革法案》的条文修正细节展开,这是丑闻被曝光之后,唯一一份由两党合作起草并临时排期、紧急加入国会立法议程的法律提案。法案宗旨规定保障美国公民的隐私权;调整棱镜实施机构——国家安全局和美国其他情报机构的监听监控权限;明确监听监控授权机构——外国情报监视法庭的职责。整个法案对美国以外的其他国家公民的权益保护只字未提,涉及对《爱国者法案》和《外国情报监视法》部分条文赋予情报机构的“超国界”监控权,国会也丝毫不打算干涉。这意味着,即使是在已经激起全球愤慨、声讨一片的境况下,以美国国家安全局为首的情报机构将一如既往地对外国公民进行雷打不动的监控。

四、法律启示

透过棱镜事件,法律界人士需要反思至少两件事情:其一,为什么棱镜监听项目在美国不算违法?毕竟,其侵害的客体对象也包括美国本土公民在内的数据隐私权利。其二,为什么各国信息安全法律、数据隐私法律,以及林林总总的国际条约和协定等浩如烟海的法律法规条文,层层设防,处处布控,却依然挡不住美国情报机构的非法入侵?

探究第一个问题,要从美国长达80多年的监听立法史说起。情报监听在美国可以追溯到1934年的《联邦通信法》,该法也是世界上第一部将情报监听纳入法律条文的成文法,其对电话窃听的证据适用作出了规定。20世纪60年代,在美国民权运动的推动下,1968年《综

合控制犯罪和街道安全法》对监听制度予以全面规范，很多的制度规定从整体上构筑了美国监听法制的基石。例如，运用监听必须经过法定机关签发令状批准；对于特定的紧迫情形可以不经法官批准而进行监听，但在监听开始后 48 小时内应申请补发监听令状……该法案所确立的监听原则和程序在此后很多年都稳如磐石，但随着美国日后反恐、对外战争等宏观形势的逐日变革，这一基石不断松动。1974 年尼克松水门事件爆发，美国国家安全部门着手拟定通信监听的单行法律。1978 年，国会通过《外国情报监视法案》，将矛头由国内转向国外，目标为“外国势力及其代理人”。法案授权司法部组成外国情报监控法庭（FISC），赋予其对美国国家安全机构情报监听进行授权令状核发，以及所谓监督权限的权力。FISC 也是本次曝光的棱镜计划的授权部门。

从 20 世纪 80 年代开始，电子通信技术迅猛发展。1986 年《电子通信隐私法》将有线通信和无线通信纳入监听范围。1994 年《执法通信辅助法》将电信运营商纳入监听行动，赋予其辅助义务。9·11 恐怖袭击之后，2001 年 10 月，《爱国者法案》火线出台，该法案从整体上改变了美国监听法制的走向。自此，美国监听法制的价值体系开始向反恐和保护国家安全倾斜，赋予执法人员更大的权力，规定对于那些涉嫌从事恐怖活动者的电话监听、电子邮件和互联网跟踪，无须再获法庭批准。在反恐的大背景之下，系列法律被修正，陆续有新的网络通信服务提供商被赋予辅助监听之职，同时，监听的前置条件、启动事由等不断松懈，情报和执法部门的监听权力也在逐步扩大。2005 年《通信协助执法法案》（修正案）将宽带和网络电话服务提供商（VoIP）纳入规制范围，要求其承担与电信运营商类似的辅助监听义务。2006 年 3 月，《美国爱国者法修改与再授权法》和《爱国者法额外再授权修改法》共同对《爱国者法案》的重要章节予以永久化，并通过延长搜查令状的期限、增加可以监听的犯罪类型、修改条款的效力期限等方式加强了执法部门权限。2008 年 7 月，《外国情报监视法》（修正案）规定，在未经 FISC 批准的前提下，情报机构可先期对嫌疑人采取监听

措施。

通过以上回顾可知，在美国，无论是监听的启动事由、对象，还是监听的程序，棱镜的实施都可以从美国现有成文法律条文中找到依据。而从美国国会近几年的立法提案来看，美国情报机构的监听权限还有持续扩充的趋势，在以反恐和保障国家安全的价值路标面前，众多个人权利保护的屏障也将被悉数卸下。以2008年提出《网络情报分享和保护法案（草案）》（下称“CISPA”）为例，其中规定除以“网络安全”和“国家安全”等事由启动监听外，拟新增三条启动监听的事由，即“对网络犯罪行为的调查和起诉”、“保护个人”、“保护儿童”，美国国内法律界普遍认为，一旦草案通过，情报机构的监听权限将无限扩大，写在法条中的所谓公民权利也将自此灭失。

对于第二个问题，源于美国法律文本的特色，简而言之有以下三个方面。其一，外国公民隐私权在美国法律和判例中不被承认。美国《宪法第四修正案》只保护美国公民的隐私权，外国公民不被保护。联邦判例也没有任何保护外国公民隐私权的先例。其二，法律条文有意模糊化处理，不设边界。《爱国者法案》第215条和《外国情报监视法修正案》第702条，模糊化处理核心问题，例如，获取证据信息（“Tangible Things”）的范围是“任何”（“Any”），这种模糊化处理的立法手段使得美国情报机构、执法机构可在这一地带任意游走。其三，法律条文中的涉外定义一般倾向于政治化处理。凡是与美国国家安全、反恐等相关的事宜，只要涉外，一般都政治化处理，例如，《外国情报监视法修正案》中对于“外国情报信息”（“Foreign Intelligence Information”）的定义，规定为：“外国政府、机构……可能实施的……潜在的……”欧洲议会发布的《美国情报监听项目及其对欧洲公民基本权利的影响》中认为，这不是法律而是政治。

棱镜事件所折射出的各国现有法律问题，已经远远超出信息安全这一单一领域本身。目前看来，至少还有跨境数据流动规则、公民数

据隐私保护、网络服务提供商（含通信、互联网企业）的义务责任、网络空间法律规则等诸多议题亟待反思，尤其是，除了传统惯性思维所应当考虑的是否还有法律空白需要填补之外，更重要的关注点应该是，现有法律在执行上是否彻底，法律规则是否真的有效，法律条文能否切实保障公民的各项权益。最后，面对棱镜所折射的美、英等国在网络空间领域的绝对霸权，应有什么样的法律条文才能与之相对抗，筑起我们在该领域的坚固防线。

第五篇

案例篇



第十六章 我国互联网相关司法案例概述

2013 年，与互联网具有强相关关系的民商经济案件有 140 余件，这些案件大部分为知识产权纠纷，特别是著作权（信息网络传播权）纠纷，少数为不正当竞争、滥用市场支配地位和合同纠纷。涉案标的多数为视频（含电影、电视剧和以类似摄制电影的方法创作的作品），少数为计算机软件、商标。

本书通过对 2013 年度的司法诉讼案例进行梳理，汇总了 22 件有代表性的、与互联网具有强相关关系的司法案例，并将其作为分析研究的主要对象。案例有关情况概述如下。

一是从案件发生地域看，互联网领域的诉讼案件主要发生在北京市（18 件）和广东省（3 件）两地，主要集中在北京市。这与互联网企业主要分布在该地域有关。

二是从作出判决法院的层级看，主要集中在中级人民法院（8 件）和初级人民法院（9 件）。这主要与相关案例主要是著作权或者信息网络传播权纠纷、争议标的额不大有关。

三是从案由看，绝大多数是著作权纠纷案件（19 件），少数是商标权和不公平竞争纠纷案件（2 件）、滥用市场支配地位纠纷案件（1 件）。这主要与互联网的平台性有关。互联网承载着诸多内容应用，现实生活中易产生的纠纷，在互联网领域也易发生。但是，近年来直接与互联网服务本身有关的纠纷，如不正当竞争、干扰服务等时有发生，如 3Q、3B 纠纷等，引起了社会各界的广泛关注，有些纠纷还进入了司法程序。

根据梳理,互联网领域案例主要有如下特点。

一是在具体审理案由上,多数为信息网络传播权等著作权纠纷案件,少数为不正当竞争案件。在信息网络传播权纠纷案件中,典型的侵害行为主要为互联网经营者未经权利人许可通过播放平台、API平台、手机播放器或者硬件设备使用他人作品^①。多数网络纠纷案件的违法行为与互联网本身的特点结合并不紧密。

二是在有些案例中,若干涉诉行为与互联网本身特点有关,为司法审判增加了新的研究领域。例如,信息网络传播权授权的范围是否可以扩展为被授权人域名的子域名系统,就是互联网本身特点带来的新课题,北京市第一中级法院从保护著作权出发,倾向认为作品授权使用范围并不当然延伸至子域名系统^②。

三是在有些与互联网特点有关行为定性上,审判者似乎未能充分考虑到互联网技术性强、发展迅速的特点,而较为保守地适用有关规定。例如,关于通过播放软件向公众播放来自第三方网站的作品行为,是否为直接提供作品内容的在线播放行为,有案例认为播放软件仅提供了搜索、链接服务,而非提供在线播放行为,属于非侵害信息网络传播权的行为^③。关于通过链接、搜索提供第三方网站提供的作品的行为,应考虑到互联网技术上完全可以实现不改变第三方提供的作品,而通过链接、搜索服务向公众提供侵权作品的可能性。

四是由于互联网平台性和开放性的特点,主要针对传统社会的判

① 参见北京市朝阳区人民法院民事判决书(2012)朝民初字第33384号、北京市第一中级人民法院民事判决书(2013)一中民终字第5033号、北京市朝阳区人民法院民事判决书(2013)朝民初字第15964号、北京市第一中级人民法院民事判决书(2013)一中民终字第8328号。

② 参见搜狐与乐视的相关诉讼案件,如北京市第一中级人民法院民事判决书(2013)一中民终字第05463号、北京市第一中级人民法院民事判决书(2013)一中民终字第05037号、北京市第一中级人民法院民事判决书(2013)一中民终字第7642号。

③ 参见北京市朝阳区人民法院民事判决书(2013)朝民初字第15308号。

断规则和认识规则发生了变化。例如，对于互联网领域是否具有竞争关系的认定，则不再局限于双方提供的产品或者服务是否相同、相近或者有替代关系，而是更广泛地认定互联网服务提供者之间具有竞争关系，即使二者之间提供的产品或者服务完全不同^①；关于相关地域市场的界定，并不简单将地域限定为本国国内，而是考虑互联网的互通性和开放性，将地域市场范围扩展到其他地域^②。

近年来发生的互联网领域司法案例主要表现为互联网内容服务纠纷，但与互联网服务及互联网本身特点有关的案例也在逐渐增多。这是我国互联网服务市场日渐发达、繁荣的结果。具体而言，司法案例有如下趋势：

一是互联网本身的特点将逐步产生新的纠纷类型，或者改变、丰富原有纠纷的行为模式，为司法审判带来新的课题。

二是互联网的发展，将促使不断研究传统规则在互联网领域的适用问题，或者将产生新的规则。从相关案例可以看出，审判者注意到互联网领域的特点，主动研究解决新问题，并未固执、保守地沿用适用于传统社会的规则。

三是互联网行业与司法的互动性将加强，司法对互联网规则的影响将逐步显现。例如，关于对互联网经营行为规范和有关服务行为的判断，法院主动运用行业主管部门的规章和协会自律规范作为依据和论据，支撑自己的判断^③。对于用户是否可以利用第三方服务屏蔽广告一事，相较于行业主管部门和互联网行业的暧昧态度，法院鲜明地认为：“用户若想享有免费的即时通信服务，就必须容忍广告和其他推销增值服务的插件和弹窗的存在。那种不愿意通过交费来使用无广告、

① 参见北京市第一中级人民法院行政判决书（2012）一中民初字第5718号。

② 参见广东省高级人民法院民事判决书（2011）粤高法民三初字第2号。

③ 参见广东省高级人民法院民事判决书（2011）粤高法民三初字第1号。

无插件的互联网服务，而通过使用破坏网络服务提供者合法商业模式、损害网络服务提供者合法权益的软件来达到既不浏览广告和相关插件，又可以免费享受即时通信服务的行为，已超出了合法用户利益的范畴”，认为网络服务提供者不可以“假借查杀病毒或者保护用户利益之名，侵入其他网络服务提供者合法软件的运行进程，通过擅自修改他人软件的手段达到破坏他人合法经营的目的”^①。

① 参见广东省高级人民法院民事判决书（2011）粤高法民三初字第1号。

第十七章 典型法律问题分析

一、关于作品授权使用范围是否自动延及被授权方网络平台的子域名系统

在搜狐新媒体公司与乐视公司一系列侵犯著作权纠纷案件中^①，双方争议的焦点是：乐视公司与搜狐新媒体公司签订的《非独家信息网络传播权采购协议》允许搜狐新媒体公司在“www.sohu.com”网站在线播放涉案电视剧的授权，是否可以延及该网站的子域名系统，例如其与爆米花公司合作的“baomihua.tv.sohu.com”网站、其与“MSN 中国”合作的“msn.tv.sohu.com”网站和其与飞狐公司及三基公司合作的“boosj.tv.sohu.com”网站。

关于该争议，搜狐新媒体公司认为其获得了涉案电视剧或者电影《将爱情进行到底》、《野鸭子》和《一夜未了情》等的信息网络传播权，其与乐视公司签订的《非独家信息网络传播权采购协议》约定其可以在“www.sohu.com”网站在线播放，其在“baomihua.tv.sohu.com”、“msn.tv.sohu.com”或者“boosj.tv.sohu.com”在线播放，均是在搜狐新媒体公司经营的搜狐视频的域名 tv.sohu.com 下使用，不构成侵权，且其与第三方合作的网站上的内容全部来源于其自身的服务器，涉案影片或者电视剧的使用者为搜狐新媒体公司自身，而非第三方，故其使用行为未超出其与乐视公司协议约定的范围。

^① 参见北京市第一中级人民法院民事判决书（2013）一中民终字第 05463 号、北京市第一中级人民法院民事判决书（2013）一中民终字第 05037 号、北京市第一中级人民法院民事判决书（2013）一中民终字第 7642 号。

法院审理认为,《非独家信息网络传播权采购协议》的授权范围并不应包括搜狐新媒体公司与他人合作经营的网络平台。除此之外,由于搜狐新媒体公司与乐视公司签订的《非独家信息网络传播权采购协议》约定,涉案影片的授权使用范围仅限于 www.sohu.com, 未经乐视公司书面许可, 搜狐新媒体公司不得通过任何方式, 包括转许可本合同以外的第三方, 或与其合作而使其超链接、深层链接、播放器嵌套, 或共同设立合作频道使用作品。搜狐新媒体公司通过对其与第三方合作的网络平台提供涉案影片的在线播放的行为, 已经超出乐视公司对搜狐新媒体公司的授权范围, 应承担侵权责任。

由于争议双方已签订协议, 搜狐新媒体在其与第三方合作平台上使用涉案作品是否超出授权范围, 应首先根据协议的约定进行判断。但如果双方协议未明确禁止被授权方与第三方合作使用涉案作品, 法院应如何判决? 从法院审理查明的事实看, 搜狐新媒体公司与第三方合作经营的“baomihua.tv.sohu.com”、“msn.tv.sohu.com”和“boosj.tv.sohu.com”均由搜狐新媒体公司经营管理, “baomihua.tv.sohu.com”、“msn.tv.sohu.com”和“boosj.tv.sohu.com”均是“sohu.com”的子域名, 是“www.sohu.com”网站的组成部分。因此, 在形式上, 搜狐新媒体公司在“baomihua.tv.sohu.com”、“msn.tv.sohu.com”和“boosj.tv.sohu.com”使用涉案作品, 或者在“tv.sohu.com”（乐视公司认可在该平台的使用）使用涉案作品, 均是在“www.sohu.com”网站范围内, 未超出授权范围。如果认为涉案作品仅限于在“tv.sohu.com”使用, 一则双方协议未明确限定在“tv.sohu.com”使用涉案作品, 二则也会限制被授权方的网站发展。因此, 如果没有第三方因素介入, 搜狐新媒体公司在“baomihua.tv.sohu.com”、“msn.tv.sohu.com”和“boosj.tv.sohu.com”或者其他子域名系统使用涉案作品, 均未超出授权范围。

综上, 前述情形下争议的核心点并非“baomihua.tv.sohu.com”、“msn.tv.sohu.com”和“boosj.tv.sohu.com”是否为“www.sohu.com”的子域名

或者子系统，而是第三方因素的介入，即搜狐新媒体公司与第三方利用合作经营方式使用涉案作品，超出了乐视公司的授权范围。在解释上，如无明确约定，作品的授权使用范围均应是有限的而非无限制的。乐视公司就涉案作品的授权使用人是搜狐新媒体公司，而搜狐新媒体公司与第三方合作使用涉案作品即扩大了使用主体范围，显然超出了授权范围。因此，判断互联网领域使用作品的范围是否超出授权，不应当看使用的平台是否归属于双方约定的网络平台，而应看使用主体、使用方式等是否超出约定范围。

二、关于用户是否可以卸载、屏蔽互联网服务者提供的广告等正当服务

近年来，有些网络服务提供者利用用户的同意或者假借用户的授权，干扰、卸载或者屏蔽其他网络服务提供者服务的现象时有发生，有些事件影响较大，引起了社会广泛关注。那么，用户的“同意”或者授权是否为干扰其他网络服务的挡箭牌？换言之，用户的选择权是否无限制？

网络服务提供者是否可以借口保护用户权益或者借助用户同意而干扰、屏蔽、卸载其他网络服务提供者的服务，与用户的选择权是否无限制，是一个问题的两个方面，核心是用户权益与网络服务提供者权益之间的边界。

面对网络服务提供者利用用户的同意或者假借用户的授权，干扰、卸载或者屏蔽其他网络服务提供者服务的现象，行政主管部门的态度似乎并不明确，在专门规范互联网信息服务规则的《规范互联网信息服务市场秩序若干规定》中，仅是禁止“欺骗、误导或者强迫用户使用或者不使用其他互联网信息服务提供者的服务或者产品”，而对于利用用户自愿选择同意后屏蔽广告等服务的行为是否合理未置可否。行政主管部门未明确其态度，似乎与用户因素的介入有关。根据《消

消费者权益保护法》的规定，用户享有“自主选择商品或者服务的权利”。如果限制用户屏蔽、卸载广告等服务，似乎会限制用户选择权，将会广受社会诟病。但是任何权利都是有边界的，用户选择权的边界在哪里，需要结合互联网的商业模式进行判断。

在“腾讯科技（深圳）有限公司（原告）等诉北京奇虎科技有限公司（被告）等不正当竞争纠纷案”中，审理法院对原告的商业模式进行了分析，认为原告的商业模式是向用户提供免费的即时通信服务，然后再借助即时通信软件搭建的平台向用户提供网络社交、资讯、网游、娱乐等增值服务，并为广告客户投放商业广告，实现赢利。原告所采取的在免费即时通信服务平台上开展营利业务（广告+增值服务业务）及推广其他产品和服务的商业模式，系当前国际国内即时通信行业的商业惯例。由于用户在享受即时通信服务的时候没有支付相关费用，因此花费一定的时间浏览广告和其他推销增值服务的插件和弹窗，是其必须付出的时间成本。用户若想享有免费的即时通信服务，就必须容忍广告和其他推销增值服务的插件和弹窗的存在。在这里，审理法院认可了互联网向用户免费提供服务通过广告进行营利的商业模式的合理性。进而认为“那种不愿意通过交费来使用无广告、无插件的互联网服务，而通过使用破坏网络服务提供者合法商业模式、损害网络服务提供者合法权益的软件来达到既不浏览广告和相关插件，又可以免费享受即时通信服务的行为，已超出了合法用户利益的范畴。长远来看，因为QQ平台上的增值和广告业务发展得越好，研发资金越充裕，则提供给用户的免费即时通信服务将越优质和越持久”。

在此分析的基础上，审理法院合理区分了广告、游戏和病毒、木马的不同，认为“腾讯在即时通信平台上发布的广告、游戏及增值服务不属于病毒、木马程序和流氓软件，被告无权假借查杀病毒或者保护用户利益之名，侵入其他网络服务提供者合法软件的运行进程，通过擅自修改他人软件的手段达到破坏他人合法经营的目的。被告一方

面在自己的平台上开展综合性服务，投放广告、提供新闻弹窗服务及设置其他产品和应用的入口、开展增值服务；另一方面又以保护 QQ 用户安全为名，提供工具鼓励和诱导用户过滤原告的广告和资讯服务、删除和破坏原告的增值服务和 QQ 的其他功能和服务，违背了诚实信用和公平竞争原则，具有明显的不正当竞争的恶意，是导致“3Q”大战爆发的根本原因，被告的上述行为严重损害了互联网经营秩序。审理法院最终认为，被告认为其只是给 QQ 用户提供了技术中立的修改工具，并不构成侵权的主张不能成立。

在上述案件中，审理法院详细论述了互联网免费服务商业模式的合理性，并在此基础上界定了用户的权利边界，即用户的权利边界应当符合正当互联网商业模式的良性发展需求，不应破坏服务提供者与用户之间的利益平衡。对于网络服务提供者提供的正当服务，用户的选择权并非是无限制的。虽然该案尚是个案，但其对互联网用户选择权进行了明确和合理的界定，将会对互联网行业发展产生深远影响。

三、关于搜索链接服务的免责边界问题

根据《著作权法》的规定，著作权人享有信息网络传播权，即以有线或者无线方式向公众提供作品，使公众可以在其个人选定的时间和地点获得作品的权利。简言之，信息网络传播权是将作品在网络中播放的权利。如果未经授权，而在网络中播放他人作品即属侵权。《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第四条明确规定提供作品的“搜索、链接”服务不属于侵害信息网络传播权，即提供链接、搜索的行为不属于播放作品的行为。

在北京搜狐新媒体信息技术有限公司（原告）诉北京风网信息技术有限公司（被告）侵害作品信息网络传播权纠纷案中^①，被告通过其

经营的“100TV 播放器”手机端提供原告享有信息网络传播权的涉案电视剧的全集播放，法院审理认为，被告就涉案“100TV 播放器”软件在线播放涉案电视剧提供的是搜索、链接服务，并非由其服务器直接提供了涉案电视剧的在线播放行为，且原告并未在诉前通知被告停止链接，判决被告不承担直接侵权责任。法院判决被告不承担侵权责任，在于被告提供的是链接搜索服务，而非直接在线播放行为。

被告研发的“100TV 播放器”为视频播放软件，可以在手机终端上运行，并可以通过连接互联网在线播放涉案电视剧。审理法院查明，在通过“100TV 播放器”查找涉案电视剧的过程中，在搜索结果中涉案电视剧播放图标中确实存在“来源优酷”的字样。如果认定被告提供的仅是全网的搜索链接服务，被告并不承担直接侵权责任，而仅能就其提供的搜索链接服务在避风港原则下承担相关责任。

但是，考虑到互联网技术发展迅速，如果有网络服务商利用提供搜索链接的形式定向向用户提供作品，且对用户而言其提供的搜索、链接服务与其他网络服务商直接提供的播放服务无异，是否应恪守“搜索链接服务不承担直接侵权责任”规则？这里应当探讨如下问题：①搜索链接是否仅是网络服务商向用户提供作品的形式或者方式，其真正目的是不是定向向用户提供作品，尽管其不向用户收费；②如果认为前述情形下网络服务商向用户提供的服务的本质是搜索链接，不需要承担直接侵权责任，是否会导致该情形下的网络服务商不需要取得授权即可向用户提供作品，会鼓励其他服务商选用该种提供作品的方式，进而不利于著作权保护。

搜索、链接服务提供商与内容版权方并非完全对立的关系，如果不加区别地从法律上对搜索、链接服务提供商施加过度的注意义务，或者对其完全不加限制，都将导致双方的权利与义务失衡。如何认定

① 参见北京市朝阳区人民法院民事判决书（2013）朝民初字第15308号。

搜索、链接服务提供者的侵权责任，一直是学术界、实务界争议颇多的问题。而且，随着新型互联网技术的普及和商业模式的不断创新，这一认定必将愈加复杂。我们应坚持的原则是：仅提供搜索、链接服务不构成直接侵权行为，但在符合特定要件的情况下构成共同侵权行为，问题主要集中体现在主观过错的认定。搜索、链接服务提供者是否具有主观过错，要结合个案中的搜索、链接服务提供方式与搜索、链接服务提供商的主观认知义务综合认定。

第十八章 典型案例判决要点

一、中国互联网新闻中心诉北京市盛世阳光文化传播有限责任公司等侵犯著作权纠纷案^①

法院审理认为：依据涉案 40 个访谈节目的署名情况，可以认定中国互联网新闻中心（原告）是涉案 40 个访谈节目的制作者。关于涉案 40 个访谈节目的性质，结合节目形式及制作过程来看，虽然所有节目均添加了标识及字幕，部分节目还穿插了作品展示或活动现场展示等内容，但受访谈节目本身形式的制约，采访方式基本为问答式，机位或镜头切换较少，制作者在拍摄、剪辑、加工等方面能够作出的表达非常有限，未能达到作品所要求的独创性高度。因此，根据《中华人民共和国著作权法实施条例》的有关规定，认定涉案 40 个访谈节目系电影作品和以类似摄制电影的方法创作的作品以外的任何有伴音或者无伴音的连续相关形象、图像的录像制品。中国互联网新闻中心作为涉案 40 个访谈节目的制作者，依法享有包括信息网络传播权在内的录像制作者权。

盛世阳光公司（被告一）注册了域名 ieshu.com.cn，肖延宇（被告二）注册了域名 ieshu.com，通过这两个域名均可以访问“中国美术网”，故盛世阳光公司与肖延宇系“中国美术网”的所有者和经营者。盛世阳光公司与肖延宇在“中国美术网”向公众提供涉案 40 个访谈节目的在线播放，侵犯了中国互联网新闻中心依法享有的信息网络传播权，应当承担停止侵权、赔偿损失等法律责任。

^① 参见北京市朝阳区人民法院民事判决书（2012）朝民初字第 33384 号。

二、北京搜狐互联网信息服务有限公司等与乐视网信息技术（北京）股份有限公司侵犯著作权系列纠纷案^①

法院审理认为：乐视公司（被上诉人）独占享有对涉案电视剧的信息网络传播权。根据乐视公司向原审法院提交的证据显示，涉案电视剧系在域名为 baomihua.tv.sohu.com^② 的网页中通过选择涉案电视剧而播放的，该页面左上角显示“爆米花网”，在涉案电视剧播放过程中，视频左上角始终显示“搜狐视频 tv.sohu.com”字样，视频右下角也显示“搜狐视频”。

乐视公司将涉案电视剧的非独家信息网络传播权授予搜狐新媒体公司（上诉人一），许可权利的范围仅限于在 www.sohu.com 网站上播放，未经乐视公司书面许可，搜狐新媒体公司不得通过任何方式，包括转许可本合同以外的第三方，或与其合作而使其超级链接、深层链接、播放器嵌套，或共同设立合作频道，以使其得以直接使用涉案电视剧。而本案中，搜狐公司通过与爆米花公司（上诉人二）设立合作平台提供涉案电视剧的在线播放，显然已超出乐视公司对搜狐新媒体公司的授权范围，故搜狐公司关于其未超授权范围使用的上诉理由没有事实和法律依据，本院不予支持。

搜狐公司还主张涉案网站的 IP 地址足以认定涉案电视剧的播放系存在于爆米花公司的服务器上，爆米花公司系通过技术手段获取搜狐公司 API 平台上的涉案电视剧，应自行承担责任。对此本院认为：首先，仅凭涉案网站的 IP 地址尚不足以证明涉案电视剧存储于爆米花公司的服务器中。其次，搜狐公司提交的证据尚无法证明其与爆米花公司的

^① 北京市第一中级人民法院民事判决书（2013）一中民终字第 5032 号、北京市第一中级人民法院民事判决书（2013）一中民终字第 5033 号、北京市第一中级人民法院民事判决书（2013）一中民终字第 5034 号、北京市第一中级人民法院民事判决书（2013）一中民终字第 05462 号、北京市第一中级人民法院民事判决书（2013）一中民终字第 05463 号。

^② 其他三件案件中，涉案电视剧可以在“msn.tv.sohu.com”播放。

合作过程中存在所谓“独家剧”与“非独家剧”使用权限的区分。再次，搜狐公司提交的证据并不能证明爆米花公司存在通过技术手段获取搜狐公司 API 平台上的涉案电视剧的行为。因此，搜狐公司关于侵权责任应由爆米花公司承担的上诉理由没有事实和法律依据，本院不予支持。

三、北京搜狐新媒体信息技术有限公司诉北京风网信息技术有限公司侵害作品信息网络传播权纠纷案^①

法院审理认为：搜狐公司（原告）享有涉案电影被授权期限内的信息网络传播权，其有权单独提起本案诉讼。本案中，“100TV 播放器”系风网信息公司（被告）研发的视频播放软件，在手机终端上运行该软件通过连接互联网可以在线播放涉案电视剧。

根据本案查明的事实，考虑到风网信息公司在公证影视作品内容来源的公证过程中，能够还原上述跳转至优酷播放页面的播放过程，同时结合下述三点理由：第一，在通过“100TV 播放器”查找涉案电视剧的过程中，在搜索结果中涉案电视剧播放图标中确实存在“来源优酷”的字样；第二，风网信息公司诉讼中对涉案电视剧来源公证时通过 WireShark 软件显示的数据来源信息中确实包括“youku”字段；第三，搜狐公司并未举证证明其诉前就涉案侵权事宜通知过风网信息公司，风网信息公司在取证后亦断开了相关侵权链接的情况，本院综合认定搜狐公司现有证据不足以证明风网信息公司通过其服务器直接提供了涉案电视剧的在线播放行为，风网信息公司就涉案“100TV 播放器”软件在线播放涉案电视剧提供的是搜索、链接服务。因此，搜狐公司要求风网信息公司承担赔偿责任损失及合理支出的直接侵权责任，没有事实和法律依据，本院不予支持。

^① 北京市朝阳区人民法院民事判决书（2013）朝民初字第 15308 号。

四、黄铁鹰等与合一信息技术（北京）有限公司侵害著作权纠纷上诉案^①

法院审理认为：《中华人民共和国著作权法》第十条第一款第（一）项规定：“发表权，即决定作品是否公之于众的权利”。“公之于众”是指将作品向不特定公众公开，作品是否发表并不取决于不特定的公众实际获得了该作品，而在于不特定公众是否具有获得该作品的可能性，因此，只要作品处于被不特定公众获得的状态，该作品即被发表。

虽然黄铁鹰、梁钧平（上诉人）的涉案作品仅针对北京大学 MBA 学生讲授，授课对象具有一定的特定性，但黄铁鹰、梁钧平知晓北京大学商学网教育有限公司对涉案作品进行现场录制的事实，并认可录制的目的是为日后北京大学光华管理学院教学所用，而北京大学光华管理学院教学的对象属于不特定公众，据此可以认定涉案作品已处于被不特定公众获得的状态，且该状态并未违背黄铁鹰、梁钧平的意志。因此，原审法院有关涉案作品已经发表的认定结论正确。

根据本案查明的事实，在“优酷网”搜索结果页面点击相应结果进入播放页面后，播放页面均显示了上传者信息，且合一公司（被上诉人，优酷网经营者）在“优酷网”的网站介绍中明确标示该网站为网络用户提供信息存储空间服务，黄铁鹰、梁钧平并不否认含有涉案作品的视频文件系网友上传到“优酷网”，也未提交证据证明含有涉案作品的视频系合一公司上传或者以其他方式置于向公众开放的网络服务器中。因此，合一公司就涉案视频而言仅提供了信息存储服务行为。

《信息网络传播权保护条例》第二十二条规定：网络服务提供者作为服务对象提供信息存储空间，供服务对象通过信息网络向公众提供作品、表演、录音录像制品，并具备下列条件的，不承担赔偿责任：（一）明确标示该信息存储空间是为服务对象所提供，并公开网络服务提供

^① 参见北京市高级人民法院民事判决书（2013）高民终字第 768 号。

者的名称、联系人、网络地址；（二）未改变服务对象所提供的作品、表演、录音录像制品；（三）不知道也没有合理的理由应当知道服务对象提供的作品、表演、录音录像制品侵权；（四）未从服务对象提供作品、表演、录音录像制品中直接获得经济利益；（五）在接到权利人的通知书后，根据本条例规定删除权利人认为侵权的作品、表演、录音录像制品。

《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第五条规定：网络服务提供者以提供网页快照、缩略图等方式实质替代其他网络服务提供者向公众提供相关作品的，人民法院应当认定其构成提供行为。前款规定的提供行为不影响相关作品的正常使用，且未不合理损害权利人对该作品的合法权益，网络服务提供者主张其未侵害信息网络传播权的，人民法院应予支持。

第八条第二款规定：网络服务提供者未对网络用户侵害信息网络传播权的行为主动进行审查的，人民法院不应据此认定其具有过错。

第十一条规定：网络服务提供者从网络用户提供的作品、表演、录音录像制品中直接获得经济利益的，人民法院应当认定其对该网络用户侵害信息网络传播权的行为负有较高的注意义务。网络服务提供者针对特定作品、表演、录音录像制品投放广告获取收益，或者获取与其传播的作品、表演、录音录像制品存在其他特定联系的经济利益，应当认定为前款规定的直接获得经济利益。网络服务提供者因提供网络服务而收取一般性广告费、服务费等，不属于本款规定的情形。

第十二条规定：有下列情形之一的，人民法院可以根据案件具体情况，认定提供信息存储空间服务的网络服务提供者应知网络用户侵害信息网络传播权：（一）将热播影视作品等置于首页或者其他主要页面等能够为网络服务提供者明显感知的位置的；（二）对热播影视作品等的主题、内容主动进行选择、编辑、整理、推荐，或者为其设立专门的排行榜的；（三）其他可以明显感知相关作品、表演、录音

录像制品为未经许可提供，仍未采取合理措施的情形。

根据上述行政法规、司法解释的规定，合一公司作为为涉案作品提供信息存储空间服务的网络服务提供者，对他人利用其服务传播的作品、表演、录音录像制品是否侵权一般不负有事先进行主动审查、监控的义务。同时，黄铁鹰、梁钧平是通过在合一公司的“优酷网”搜索框输入关键词的方式搜索到的涉案作品，涉案作品并非热播影视作品或与之相似的作品，涉案作品并未置于“优酷网”的首页或其他主要页面等能够为合一公司明显感知的位置，合一公司也未对涉案作品的主题、内容主动进行选择、编辑、整理、推荐或为其设立专门的排行榜，再结合涉案作品的类型为讲课内容，其中的讲授者、点评者、提问者及发言人众多等因素，应认定合一公司不知道也没有合理理由应当知道其服务对象上传的含有涉案作品的视频侵权。同时，合一公司在收到起诉状后，在合理期限内删除了含有涉案作品的视频。因此，原审法院认定合一公司不具有过错，其提供信息存储空间服务的行为不构成对黄铁鹰、梁钧平信息网络传播权的侵犯是正确的。

虽然含有涉案作品的视频文件在播放时有广告内容，但在案证据显示相关广告内容系随机播放，并非针对涉案作品投放，黄铁鹰、梁钧平也未举证证明合一公司获取了与涉案作品存在其他特定联系的经济利益。至于搜索结果中显示的缩略图，仅是一幅静态图片，而非涉案视频本身，并未替代提供涉案视频的其他网络服务提供者或网络用户向公众提供涉案作品，而是为方便网络用户选择搜索结果而对搜索结果的一种展示方式，不影响相关作品的正常使用，亦未不合理损害权利人对该作品的合法权益。黄铁鹰、梁钧平虽主张合一公司改变了涉案作品的内容，但并未指明改变的具体内容，也未就此提交证据。因此，黄铁鹰、梁钧平基于合一公司编辑和改变涉案作品、提供缩略图、存在投放广告行为而主张原审法院查明事实错误，以及合一公司未尽到最基本注意义务的上诉理由，均缺乏事实和法律依据，本院不予支持。

五、谷歌公司（Google Inc.）与爱思美（北京）信息科技有限公司著作权权属、侵权及不正当竞争纠纷上诉案^①

法院审理认为：本案二审争议焦点有三个。第一，谷歌公司（上诉人）的“Gmail”标识是否属于《著作权法》保护的作品；第二，2009年7月3日爱思美公司的行为是否构成擅自使用知名商品的特有名称或近似名称的不正当竞争行为；第三，原审判决中是否应当判令爱思美公司停止使用“gmail.cn”独立域名提供电子邮箱服务。

关于焦点问题一。谷歌公司的“Gmail”标识的字母选取了蓝、红、黄、绿四种色彩，第二个字母“M”与信封图形结合，使得“Gmail”标识整体上体现了谷歌公司的个性选择与判断，从审美意义上来看，具有了美术作品所要求的独创性，已构成《著作权法》所保护的作品。

关于焦点问题二。谷歌公司和爱思美公司作为信息网络行业的经营者，均提供电子邮箱服务，两家公司之间具有竞争关系。判断爱思美公司的被诉行为是否构成《反不正当竞争法》第五条第（二）项规定的不正当竞争行为，需要考虑以下三个方面：①“Gmail”是否属于谷歌公司在先使用的知名商品的特有名称；②爱思美公司是否属于善意使用“Gmail”标识；③若爱思美公司不属于善意使用“Gmail”标识，其行为是否造成相关公众的混淆、误认，从而构成不正当竞争行为。

首先，谷歌公司“Gmail”电子邮箱服务在2009年7月3日前为知名商品的特有名称，在2004年5月19日前有一定的知名度。根据本案查明的事实，谷歌公司于2004年1月推出“Gmail”电子邮箱服务，爱思美公司的涉案网站自2003年至2010年也一直提供电子邮箱服务。2002年爱思美网科技公司申请保护的软件名称为“爱思美Global电子邮箱系统”，简称“Global电邮”。根据Archive网站的记载，2003年8月28日涉案网站一的电子邮箱名称有“学子.网络”、

^① 参见北京市高级人民法院民事判决书（2012）高民终字第3337号。

“顺·网络”、“商务电邮·网络”、“欢乐邮·网络”等，即针对不同的邮箱类型有各自不同的邮箱名称，邮箱服务的域名均在“gmail.cn”域名前添加相应的前缀。2003年12月7日涉案网站一的电子邮箱名称为“多语言邮箱”或“爱思美中文邮箱”。基于上述事实，尽管爱思美公司所有的“gmail.cn”域名注册在先，但现有证据不能证明爱思美公司在该域名下提供的电子邮箱服务名称于2003年8月28日即被命名为“Gmail”。根据 Archive 网站的记载，涉案网站一于2004年5月19日将提供邮箱服务域名的前缀删除，并使用了“@gmail.cn”的邮箱名称后缀，且在此之后的网页档案保存页中出现了“北京爱思美 Gmail 邮箱系统”、“Gmail 邮件系统”、“Gmail 多语言电邮”、“Gmail 邮箱”的电子邮箱服务名称。因此，本院认定爱思美公司将其电子邮箱服务名称命名为“Gmail”的时间为2004年5月19日，谷歌公司先于爱思美公司使用了“Gmail”电子邮箱服务名称。爱思美公司关于其对“Gmail”电子邮箱名称拥有在先权利的上诉理由，缺乏事实依据，不能成立。

“Gmail”作为电子邮箱服务名称可以与其他电子邮箱服务相区分，根据谷歌公司对其“Gmail”电子邮箱服务名称知名度情况的举证，同时考虑到电子邮箱服务作为日常计算机网络服务具有的普遍性、跨地域性、传播迅速性等特点，可以认定谷歌公司的“Gmail”电子邮箱服务在2009年7月3日已经在中国大陆境内构成知名商品的特有名称。由于谷歌公司起诉解决的是2009年7月3日爱思美公司的行为是否构成不正当竞争行为，故谷歌公司对该时间点“Gmail”构成知名商品的特有名称负有举证责任。原审判决仅是对被诉行为发生时即2009年7月3日，谷歌公司的“Gmail”电子邮箱服务构成知名商品的特有名称持肯定态度，对2004年5月19日谷歌公司的“Gmail”电子邮箱服务认定其具有一定的知名度，并未明确此时谷歌公司的“Gmail”电子邮箱服务已经构成知名商品的特有名称。爱思美公司关于原审判决错误认定谷歌公司的“Gmail”电子邮箱服务在2004年5月19日构成知名

商品的特有名称的上诉主张，系对原审判决理解有误，本院不予支持。

其次，爱思美公司在涉案网站一、二中使用“Gmail”标识不属于善意使用。谷歌公司自2004年4月1日推出“Gmail”电子邮箱服务之后即获得相关公众的关注。截至2004年5月19日，该服务在电子邮箱服务领域已获得了广泛的关注和报道，由于爱思美公司在该日将电子邮箱服务名称变更为“Gmail”，原审判决结合谷歌公司的举证认定谷歌公司的“Gmail”电子邮箱服务在2004年5月19日经过短期的大量宣传已经具有一定知名度并进而认定爱思美公司作为提供电子邮箱服务的互联网企业应当知晓，其将电子邮箱服务名称变更为“Gmail”具有搭便车之故意并无不妥。且在此时间之后，爱思美公司于2004年12月还在涉案网站一的页面中使用与“Gmail”标识相近似的标识。2006年爱思美公司又在涉案网站一设置“Gmail 中国社区”栏目。2009年爱思美公司将涉案网站一、二的中文网站名称命名为“Gmail 中国”，且在涉案网站二介绍其邮箱服务时使用了“Gmail 中国全新推出基于谷歌技术的 Gmail 企业邮局正式上架销售了”等表述并使用了谷歌公司的“Gmail”标识。基于上述事实，自2004年5月19日开始至被诉侵权行为发生之时，伴随着谷歌公司“Gmail”电子邮箱服务知名度的提高，爱思美公司在持续提供电子邮箱服务中未采取一定行为与谷歌公司的“Gmail”电子邮箱服务相区分，而是使用了与谷歌公司“Gmail”标识相近似的标识、相同的邮箱服务名称，并实施了虚假宣传行为。因此，爱思美公司尽管合法拥有“Gmail.cn”的域名，但其在该域名下提供电子邮箱服务中并非善意使用“Gmail”标识，而是主观上具有搭便车之故意。

最后，爱思美公司在电子邮箱服务中使用“Gmail”标识的行为已经造成了相关公众的混淆。根据谷歌公司的举证，涉案网站一的论坛中已经有网友将爱思美公司的邮箱服务误认为是谷歌公司的“Gmail”电子邮箱服务。爱思美公司的被诉行为已经构成《反不正当竞争法》

第五条第（二）项规定的擅自使用他人知名商品特有的名称或者使用与知名商品相近似名称的不正当竞争行为。爱思美公司关于其对“Gmail”邮箱、“Gmail 中国”标识的使用是正当商业使用行为的上诉主张不能成立，本院不予支持。

关于焦点问题三。原审判决认为基于谷歌公司“Gmail”电子邮箱服务目前所具有的较高知名度，爱思美公司在使用“gmail.cn”域名提供电子邮箱服务时，即便不将该邮箱服务命名为“Gmail”邮箱，亦可能产生与谷歌公司的“Gmail”邮箱服务相混淆的后果，爱思美公司在继续使用“gmail.cn”域名提供电子邮箱服务时有义务加注区别性标识，以使消费者将两者的电子邮箱服务相区分。因此，原审判决基于爱思美公司对“gmail.cn”域名在先注册使用而允许其继续使用该域名提供电子邮箱服务，但由于爱思美公司的被诉行为构成不正当竞争行为，其不得继续在提供电子邮箱服务时使用“Gmail”标识、“Gmail 中国”的网站名称，且在提供电子邮箱服务时应在网站中附加区别性标识，使相关公众在使用爱思美公司“gmail.cn”域名下的电子邮箱服务时不会发生混淆误认，原审判决并非赋予爱思美公司在域名中有附加区别性标识的义务以避免相关公众混淆。谷歌公司关于在判决主文中应依法改判支持爱思美公司停止使用“gmail.cn”独立域名提供电子邮箱服务的上诉主张，系对原审判决理解有误，本院不予支持。

六、北京君和天下咨询有限公司诉北京掌中浩阅科技有限公司侵害作品信息网络传播权纠纷案^①

法院审理认为：我国著作权法规定，如无相反证据，在作品上署名的公民、法人或者其他组织视为作者。根据《天地民心》图书的署名情况、朱秀海与中作华文公司签署的《数字作品合作合同》以及中作华文公司出具的《声明》，可以确认君和天下公司（原告）获得了

^① 参见北京市朝阳区人民法院民事判决书（2013）朝民初字第 15964 号。

作品《天地民心》在授权期限内的独家信息网络传播权，其有权以自己的名义进行维权。

掌中阅读公司（被告）通过 iReader 安卓版手机阅读软件向用户收费提供了《天地民心》电子书的在线下载服务，其虽然表示已经获得了案外人英特颂公司的合法授权，但是首先，君和天下公司表示在涉案公证取证时朱秀海未曾将涉案图书《天地民心》的信息网络传播权授予英特颂公司，掌中阅读公司亦未举证证明英特颂公司就涉案作品已经获得了权利人的合法授权。其次，掌中阅读公司在提供收费下载涉案作品的同时，未审查英特颂公司涉案作品权利的来源，其本身亦存在过错。综上，本院认定掌中阅读公司通过 iReader 安卓版手机阅读软件向用户收费提供《天地民心》电子书的在线下载服务并未获得合法授权，侵害了君和天下公司对涉案作品《天地民心》享有的独家信息网络传播权，应当承担停止侵权并赔偿经济损失和合理支出的民事责任。

七、北京百度网讯科技有限公司等诉北京奇虎科技公司等侵犯商标权及不正当竞争纠纷案^①

法院审理认为：一、关于被告（奇虎公司）主张原告（百度公司）公证书记录的事实存在作假可能的主张是否成立

本案中，被告主张在计算机 hosts 文件被修改后，页面访问内容的真实性存在作假可能。对此本院认为，首先，原告指控的被告行为系在公证员的监督下，使用公证处提供的计算机进行固定的，且多个类似行为由多家公证处分别进行公证，虽然在计算机科技高度发展和普及的今天，对 hosts 等文件进行特别设置可能会造成访问网页并非真实的网页，但是在本案中，在多家公证处都对类似事实进行了固定，且

^① 参见北京市第一中级人民法院行政判决书（2012）一中民初字第 5718 号。

公证书均对计算机的公证步骤进行了详细记录的情况下，应当对公证书记载的事实给予充分的信任。况且，作为相关产品或服务的提供者，被告应当对其产品或服务的内容非常了解，但在本案中，被告仅主张页面访问内容的真实性存在作假可能，并未举证证明或陈述进行相关操作后的真实内容是何情形。在此情况下，本院对于被告主张原告公证书记录的事实存在作假可能的主张不予支持。此外，其他网址导航网站是否存在调用百度搜索引擎的情况、其他安全软件提供的服务内容与本案无关，对于被告的相关主张本院不予支持。

二、关于两原告和两被告是否属于本案的适格主体

《反不正当竞争法》第二条第三款规定，本法所称的经营者，是指从事商品经营或者营利性服务的法人、其他经济组织和个人。本院认为，根据电信与信息服务业务经营许可证等证据，可以认定北京百度公司为网站 www.baidu.com 的经营者。根据当事人的陈述，加之百度在线公司将第 5916519 号商标授权北京百度公司使用、第 5916519 号商标在北京百度公司为备案经营单位的 www.baidu.com 网站上使用的事实，本院认定两原告为网站 www.baidu.com 的共同经营者。

根据本案备案信息查询件等证据，本院可以认定被告北京奇虎公司为网站 www.360.cn 的经营者。鉴于涉案版本的 360 安全浏览器和 360 安全卫士均为在网站 www.360.cn 下载，加之被告北京奇虎公司对此亦予认可，本院认定被告北京奇虎公司为涉案版本的 360 安全浏览器和 360 安全卫士的经营者。

故而，本院认定原告北京百度公司、百度在线公司与被告北京奇虎公司作为相关网站和互联网产品及服务的经营者，在该领域具有竞争关系，构成《反不正当竞争法》意义上的经营者，均为本案的适格主体。

在本案中，在案证据不能证明奇智软件公司与网站 www.360.cn、

360 安全浏览器和 360 安全卫士的关系。两原告提交的合作备忘录虽然显示，奇智软件公司在与案外人百度时代公司签订协议时表示其可以利用 360 安全浏览器和 360 安全卫士进行经营，但是该合作备忘录并未指明 360 安全浏览器和 360 安全卫士的版本，且该合作备忘录的履行期间与本案两原告主张的被控不正当竞争及商标侵权行为存在的时间并无重叠，本院根据现有证据无法认定奇智软件公司与两原告指控的不正当竞争行为或侵犯商标权的行为存在关联性，故而本院对于原告北京百度公司、百度在线公司对奇智软件公司为网站 www.360.cn、涉案版本 360 安全浏览器和 360 安全卫士经营者的主张不予支持，对于原告北京百度公司、百度在线公司针对奇智软件公司的诉讼请求予以驳回。

此外，本院驳回原告北京百度公司、百度在线公司针对奇智软件公司的诉讼请求，并不影响本院对本案的管辖权。

三、关于两原告的诉讼主张是否可以在一案中审理

本案中，两原告放弃了被告行为构成侵犯著作权的主张，仅主张被告的行为构成不正当竞争和商标侵权。其主张被告构成不正当竞争的行为分为两类，即插标行为和网址导航站劫持流量行为，且主张被告构成商标侵权的行为与其主张被告构成不正当竞争的网站导航站劫持流量行为基本重合，即原告主张被告的此类行为既构成不正当竞争，又构成侵犯商标权。在此情况下，本院在一案中针对两原告对于被告的两类行为是否分别构成不正当竞争或商标侵权一并审理并无不当，符合便于当事人诉讼，便于人民法院依法高效行使审判权的原则。故本院对于被告关于本案应当分案审理的主张不予支持。

鉴于本院已经认定原告北京百度公司、百度在线公司与被告北京奇虎公司作为相关网站和互联网产品及服务的经营者，在该领域具有竞争关系，构成《反不正当竞争法》意义上的经营者，均为本案的适

格主体，故两原告有权作为共同原告向被告主张不正当竞争。在侵犯商标权纠纷的案件中，商标权人和商标被许可使用人可以共同主张权利，故在本案中，北京百度公司和百度在线公司亦有权作为共同原告向被告主张商标侵权。

四、关于被告插标等行为是否违反《反不正当竞争法》第二条

《反不正当竞争法》第二条规定，经营者在市场交易中，应当遵循自愿、平等、公平、诚实信用的原则，遵守公认的商业道德。上述法律条文的目的在于维护市场竞争的良性发展，对于恶意采取不正当竞争行为的经营者予以制止，故而审查被告行为是否具有恶意是评判其行为是否违反上述法律的关键。

本院认为，被告的 360 安全卫士在原告网站搜索结果页面上有选择地插入了红底白色感叹号图标作为警告标识，以警示用户该搜索结果对应的网站存在风险，这一行为违反了《反不正当竞争法》第二条规定的诚实信用原则，属于不正当竞争行为。因为对于安全软件来讲，其软件要实现的目的在于向用户警示访问的网站是否具有风险，而对于搜索引擎的搜索结果页面，用户显然不太可能对每个搜索结果都进行访问。在用户点击进入搜索结果中被安全软件认定为存在风险的网站时，安全软件进行提醒、拦截等行为是正当的，符合安全软件的功能和价值，亦符合用户安装安全软件的目的。但是，在未经其他经营者许可的情况下，仅以单方的认定，即通过修改其他经营者向用户提供的网络代码的方式，在他人经营的搜索引擎服务的页面上任意进行标注，对他人向用户提供的服务内容进行了改变，该行为应当被法律予以禁止。

加之在本案中，首先，被告的 360 安全卫士有选择地仅针对原告网站搜索结果页面进行了插标，对例如 Google 的其他搜索引擎网站的结果页面却没有进行插标，即使搜索结果对应的为同一个网站，被告

的 360 安全卫士也进行了区别对待。该种区别对待的行为违反了《反不正当竞争法》第二条所规定的诚实信用原则。

其次，被告的 360 安全卫士作为安全软件，其经营模式应当向用户发出警示或保护为限。但在本案中，被告不仅进行了插标，还逐步引导用户点击安装 360 安全浏览器，其插标和引导行为系通过利用原告搜索引擎服务对其浏览器产品进行了推广，属于明显的搭便车行为。

综上，法院认定原告指控被告的插标行为违反了《反不正当竞争法》第二条，构成了对原告的不正当竞争。

五、关于被告插标等行为是否违反《反不正当竞争法》第十四条

《反不正当竞争法》第十四条规定，经营者不得捏造、散布虚伪事实，损害竞争对手的商业信誉、商品声誉。

在 360 安全卫士的弹出框中，出现了“这个网站存在为欺诈网站刊登广告的行为，您可能被诱骗访问欺诈的彩票、中奖等网站，导致银行账号密码被窃取，甚至财产损失”或类似用语，原告认为网络用户在看到这些信息后，可能误解为原告网站搜索结果页面上“存在为欺诈网站刊登广告”等行为，从而会造成相关的后果，而并非理解为搜索结果对应的网站上存在上述行为。

对此本院认为，原告虽然指控 360 安全卫士的弹出框中的文字的语义存在被误解的可能，但是在案证据中类似提示框中出现的文字更多属于无歧义的表述。且在当前的网络环境下，大部分的网络用户在看到上述提示信息后，并不会当然地误解原告网站存在“为欺诈网站刊登广告”或其他不当行为，进而对原告网站产生负面评价。况且，360 安全卫士的弹出框中的文字仅表示相关网站“有可能”会造成相关后果，并非明确认定该网站存在相关有害于网络用户的行为。故本院认为，360 安全卫士的弹出框中的文字虽然有所不当，不会造成原

告或原告网站商誉的明显贬损，被告的行为不构成对原告及原告搜索引擎服务的商业诋毁，未违反《反不正当竞争法》第十四条的规定，该行为不构成不正当竞争。

综上，对原告指控被告构成诋毁商业的不正当竞争的主张，法院不予支持。

六、关于被告网址导航站劫持流量行为是否违反《反不正当竞争法》第二条

前文已述，审查被告行为是否具有恶意是评判其行为是否违反《反不正当竞争法》第二条的关键。

首先，在原告许可的情况下，被告在其网址导航站网页上嵌入原告搜索框并无不当。但是，作为原告搜索引擎服务的一部分，下拉提示词是作为搜索引擎服务商根据其服务的内容自行制定并向用户提供的，虽然原告搜索框被嵌入被告的网址导航页，但是被告无权擅自改变原告提供给网络用户搜索引擎服务的内容，即被告无权擅自改变原告在其搜索框上向用户提供的下拉提示词。

其次，在本案中，被告擅自改变原告在其搜索框上向用户提供的下拉提示词，并且采用增加文字介绍、设置背景颜色等方式，甚至在用户设置了其他搜索方向时，依然插入了与用户设置的搜索方向关联性很小的下拉提示词，引导用户访问本不在相关关键字搜索结果中靠前位置的、甚至与用户搜索目的完全不同的被告的影视、游戏等页面，进行获得更多的用户访问量，以便谋取不正当的利益，属于明显的搭便车行为。

再次，即使点击下拉提示词，亦应当进入原告网站针对所点击的下拉提示词作为关键字的搜索结果页面。但是，在本案中，点击被告擅自插入的下拉提示词，并没有进入原告搜索引擎的搜索结果页面，而是直接进入被告的影视、游戏等页面，甚至网络用户在仅设置搜索

方向，并未输入相关关键词时也会进入被告的相关网页，该事实进一步表明被告搭便车的意图非常明显。

最后，被告行为不仅不正当地获取了相关利益，亦有可能因为引导用户更多的访问与其搜索目的完全不同的页面，从而挫伤用户继续使用原告搜索引擎服务的积极性，或者使用户对原告所提供的搜索服务的负面评价，进而对原告的经营造成不利影响。

综上，法院认定，被告网址导航站劫持流量的行为违反了《反不正当竞争法》第二条规定的诚实信用原则，其行为构成了不正当竞争，对原告指控被告网址导航站劫持流量的行为构成不正当竞争的主张法院予以支持。

七、关于被告行为是否侵犯原告商标权及违反《反不正当竞争法》第五条第一款第（三）项的规定

《反不正当竞争法》第五条第一款第（三）项规定，经营者不得采用下列不正当手段从事市场交易，损害竞争对手：（三）擅自使用他人的企业名称或者姓名，引人误认为是他人的商品。《商标法》第五十二条规定，有下列行为之一的，均属侵犯注册商标专用权：（一）未经商标注册人的许可，在同一种商品或者类似商品上使用与其注册商标相同或者近似的商标的；（二）销售侵犯注册商标专用权的商品的；（三）伪造、擅自制造他人注册商标标识或者销售伪造、擅自制造的注册商标标识的；（四）未经商标注册人同意，更换其注册商标并将该更换商标的商品又投入市场的；（五）给他人的注册商标专用权造成其他损害的。

《中华人民共和国商标法实施条例》第五十条和最高人民法院《关于审理商标民事纠纷案件适用法律若干问题的解释》第一条、第十一条进一步对《商标法》第五十二条中给他人的注册商标专用权造成其他损害的情形及类似商品和服务进行了规定和解释。上述法律、法规

和司法解释规定的内容在于禁止行为人在向他人提供商品或服务时，不正当地利用他人商标、商号等造成消费者混淆，从而增加自身的交易机会。

但是在本案中，被告在其网址导航站页面上嵌入原告搜索框系按照行业内的通行规则，系在原告许可下进行的，虽然搜索框上标注有原告商标，但在原告许可的前提下，该嵌入行为不构成对原告商标权的侵犯，亦不构成《反不正当竞争法》第五条第一款第（三）项规定的情形。

本案中虽然被告存在改变下拉提示词、用户点击选择搜索方向时跳转至被告相关内容的网页等行为，但是在互联网环境下，结合本案案情，网络用户并不会误认为正在使用的搜索服务系由被告提供，或者误认为跳转后的页面系由原告提供、属于搜索引擎服务的关联内容，也就是说，不会使消费者对服务的来源造成混淆，故而法院认定被告的上述行为不构成对原告商标权的侵犯，亦不构成《反不正当竞争法》第五条第一款第（三）项规定的情形。

诚然，被告改变下拉提示词、用户点击选择搜索方向时跳转至被告相关内容的网页等系改变原告搜索引擎服务的行为，但是上述问题系属于当事人竞争行为是否正当的范畴，法院亦在被告行为是否构成违反《反不正当竞争法》第二条规定情形的部分进行了认定，被告的上述行为构成违反《反不正当竞争法》第二条规定情形并不意味着亦对原告的商标权构成侵权或构成违反《反不正当竞争法》第五条第一款第（三）项规定的情形。

综上，对于原告指控被告行为构成对原告商标权的侵犯及违反《反不正当竞争法》第五条第一款第（三）项的规定的规定的主张法院不予支持。

八、腾讯科技（深圳）有限公司等诉北京奇虎科技有限公司等不正当竞争纠纷案^①

2013年4月3日，广东省高级人民法院审理认为：

一、关于被告扣扣保镖是否能够破坏原告QQ软件及其服务的安全性、完整性，使原告丧失增值业务的交易机会及广告收入，从而构成不正当竞争的问题

根据工业和信息化部《规范互联网信息服务市场秩序若干规定》第五条规定和《互联网终端软件服务行业自律公约》第十八条、第十九条规定，无论是互联网行政管理的部门规章还是互联网业界公认的商业道德，都禁止互联网信息服务提供者欺骗、误导或者强迫用户使用或者不使用其他服务者的服务和产品，或者恶意修改或者欺骗、误导、强迫用户修改其他服务者提供的服务或者产品参数，也禁止针对特定信息服务提供商的合法广告进行拦截。被告针对原告的QQ软件专门开发了扣扣保镖。在安装了QQ软件的电脑上安装运行扣扣保镖后，该软件就会自动对QQ进行体检，进而宣布QQ存在严重的健康问题。同时，扣扣保镖使用Hook技术挂钩LoadLibraryW函数、ColoadLibrary函数或SetWindowsPos等函数，阻止QQ.exe进程加载特定插件、扫描模块以及弹出窗口，从而屏蔽QQ软件使用的插件，清理QQ软件产生的临时、缓存文件及其他相关文件，过滤QQ软件的信息窗口，等等。另外，被告还向网络用户宣称，QQ软件存在扫描用户隐私的行为，如果网络用户点击“查看QQ扫描了哪些文件”的链接后即可调用“360隐私保护器”。扣扣保镖针对QQ软件进行所谓“体检”后给出的结论，配合奇虎公司在互联网上发布的关于QQ软件正在扫描用户隐私等不实宣称，必然会使不具备网络专业知识的网络用户陷入惶惑和恐慌，

^① 广东省高级人民法院民事判决书（2011）粤高法民三初字第1号。

产生对 QQ 软件的不信任感；再加上用户希望既要免费使用 QQ 软件提供的即时通信服务，又无须受广告和推销产品插件打扰的心态，必然会使用扣扣保镖提供的上述功能，删除 QQ 的功能插件，屏蔽 QQ 发布的广告、游戏，停止使用 QQ 提供的各种功能和服务，修改 QQ 提供给用户的安全中心功能和安全扫描功能。上述行为的后果将使原告损失广告收入、游戏收入和增值服务交易机会，给原告造成严重的经济损失；同时还将使原告的软件运行产生障碍，用户体验产生改变，给原告的企业和品牌声誉造成损害。

被告针对原告 QQ 软件专门开发的扣扣保镖破坏了原告合法运行的 QQ 软件及其服务的安全性、完整性，使原告丧失合法增值业务的交易机会及广告、游戏等收入，偏离了安全软件的技术目的和经营目的，主观上具有恶意，构成不正当竞争。

二、关于被告在经营扣扣保镖软件及其服务时，是否存在捏造、散布虚伪事实，从而构成商业诋毁的问题

根据《反不正当竞争法》第十四条规定，经营者针对特定或者特定类型的竞争对手，故意或者过失地捏造、散布虚伪事实，损害后者的商业信誉和商品声誉的，构成商业诋毁。本案中，在安装了 QQ 软件的电脑上运行扣扣保镖后，该软件自动对 QQ 进行“体检”，然后显示“体检得分 4 分，QQ 存在严重的健康问题”；“共检查了 40 项，其中 31 项有问题，建议立即修复！重新体检”等。在对产品进行评价时陈述虚假或者引人误解的事实的，就有可能构成商业诋毁。在“给 QQ 体检”中，被告结合给 QQ 打低分的行为，还宣称 QQ 会扫描用户电脑里的文件，为避免隐私泄露，用户可禁止 QQ 扫描自己的文件；将“QQ 扫描我的文件”列为危险项目，提示用户“阻止”。另外，扣扣保镖还以特别醒目的方式提示用户 QQ 存在严重的健康问题；将“QQ 安全中心”列为危险项目，提示用户“升级”，这些宣称及警示语会给 QQ 用户造成一种强烈的直观感受，如“我的 QQ 很不健康”，QQ

提供的安全中心功能“危险”。被告上述暗示和明示的说法缺乏事实依据，属于捏造和虚构。其后果会直接导致用户对 QQ 产品信任度下降，对 QQ 安全性产生担忧和恐慌，对 QQ 产品和服务产生怀疑和负面评价。其次，本案证据显示，只有在用户使用了被告给用户设置的“一键修复”功能后，用户的 QQ 软件才能取得 100 分。如一旦用户成功使用“一键修复”功能，原告借助 QQ 平台搭建的增值服务和广告业务功能就将被禁用、阻止或者清除。也就是说，只有当 QQ 特定的功能插件、自带的安全防护功能、广告、资讯弹窗被一律禁用、阻止和清除后，QQ 才能得满分。QQ 所得 100 分是用户使用了扣扣保镖进行“一键修复”的结果。给 QQ 打 100 分，其实质不是为了肯定 QQ 的产品和服务，而是为了鼓励和诱导用户使用扣扣保镖的“一键修复”功能去破坏 QQ 的产品和服务。另外，QQ 打分与原告自己对 QQ 软件用户账号的安全性打分是两种不同性质的行为。二者打分的对象不同：被告是在对 QQ 这款软件进行打分，而原告只是对 QQ 用户使用的账号密码是否安全进行打分；二者打分的目的也不同：被告的打分是为了贬低 QQ 的产品安全性和正常的功能设置，原告打分是为了善意提醒用户提高登录密码的安全等级。可见，在认定是否构成商业诋毁时，应该综合考虑所谓“打分”和经营者在“打分”过程中所发布的一系列明示或者暗示的言论将会给用户造成的影响和效果，而非孤立、割裂地看待某个“打分”行为自身是否构成商业诋毁。

综上所述，被告针对原告的经营，故意捏造、散布虚伪事实，损害后者的商业信誉和商品声誉，构成商业诋毁。

三、关于被告的扣扣保镖是否通过篡改 QQ 的功能界面从而取代原告 QQ 软件的部分功能以推销自己的产品，构成不正当竞争的问题

被告以“升级 QQ 安全中心”为名，通过“一键修复”和“保护 QQ 安全”功能限制 QQ 安全中心功能，篡改 QQ 功能界面，用被告自己的扣扣保镖运行界面取而代之。同时，被告一方面通过安全恐吓和“一键修复”、

“隐私保护”功能阻止 QQ 用于查杀木马的安全扫描功能，另一方面又在“给 QQ 体检”、“隐私保护”中强烈推荐用户安装使用 360 安全卫士的木马查杀功能。由此可见，被告以保护用户利益为名，推出扣扣保镖软件，诋毁原告 QQ 软件的性能，鼓励和诱导用户删除 QQ 软件中的增值业务插件、屏蔽原告的客户广告，其主要目的是将自己的产品和服务嵌入原告的 QQ 软件界面，依附 QQ 庞大的用户资源推销自己的产品，拓展 360 软件及服务的用户。被告在给原告造成了严重经济损失的同时推销自己的产品，增加自己的交易机会，违反了诚实信用和公平竞争原则，构成不正当竞争。

2014 年 2 月 24 日，最高人民法院就本案进行了终审判决：驳回上诉，维持原判。最高人民法院在判决中就互联网竞争的基本规则进行了明确阐释：

一、行业的竞争行为必须要符合行业惯例、诚实信用原则和公认的商业道德

最高人民法院在判决中明确指出，市场经济是由市场在资源配置中起决定性作用，自由竞争能够确保市场资源优化配置，但市场经济同时要求竞争公平、正当和有序。在市场竞争中，经营者可以根据市场需要和消费者需求自由选择商业模式，这是市场经济的必然要求。腾讯通过开发 QQ 软件，以该软件为核心搭建一个综合性互联网开放平台，并提供免费的即时通讯服务，吸引相关消费者体验、使用其增值服务，同时亦以该平台为媒介吸引相关广告商投放广告，这种免费平台与广告或增值服务相结合的商业模式是互联网行业惯常的经营方式。360 公司专门针对 QQ 软件开发、经营扣扣保镖，以帮助、诱导等方式破坏 QQ 软件及其服务的安全性、完整性，减少了腾讯的经济收益和增值服务交易机会，干扰了腾讯的正当经营活动，损害了腾讯的合法群益，违反了诚实信用原则和公认的商业道德。

二、安全软件的评测行为需善尽谨慎注意义务

最高院指出：，经营者对于他人产品、服务或者其他经营活动并非不能评论或者批评，但是评论或者批评必须有正当目的，必须客观、真实、公允和中立，不能误导公众和损人商誉。经营者为竞争目的对他人进行商业评论或者批评，尤其要善尽谨慎注意义务。360 无事实依据地宣称 QQ 软件会对用户电脑硬盘隐私文件强制性地查看，并且以自己的标准对 QQ 软件进行评判并宣称 QQ 存在严重的健康问题，造成了用户对 QQ 软件及其服务的恐慌及负面评价，使相关消费者对 QQ 软件的安全性产生怀疑，影响了消费者的判断，并容易导致相关用户弃用 QQ 软件及其服务或者选用扣扣保镖保护其 QQ 软件。这种评价已超出正当商业评论、评价的范畴，突破了法律界限，构成商业诋毁。

三、正当的市场竞争是竞争者通过必要的付出而进行的诚实竞争，损人利己构成不正当竞争

对于 360 通过扣扣保镖将 QQ 软件的安全沟通界面替换为扣扣保镖界面的行为，最高人民法院认为，360 的不正当竞争行为是一个有计划、有步骤的方案，即首先通过贬损 QQ 软件来引导用户安装扣扣保镖；在用户安装和运行扣扣保镖过程中，通过有计划的行为引导、帮助用户安装上诉人产品 360 安全卫士；并通过扣扣保镖的一键修复功能，将 QQ 软件的安全沟通界面替换成扣扣保镖界面。其根本目的在于依附 QQ 软件强大用户群，通过对 QQ 软件及其服务进行贬损的手段来推销、推广 360 安全卫士，从而增加其市场交易机会并获取市场竞争优势，此行为本质上属于不正当地利用他人市场成果，为自己谋取商业机会从而获取竞争优势的行为，构成不正当竞争。

四、互联网领域不是可以为所欲为的法外空间，技术创新和自由竞争，必须要以不侵害他人合法权益为边界

针对 360 公司认为其行为是互联网自由和创新精神的体现，一审法

院违反行业发展规律，苛刻适用反不正当竞争法的一般原则会限制竞争和打击创新的说法，最高人民法院指出：互联网的发展有赖于自由竞争和科技创新，互联网行业鼓励自由竞争和创新，但这并不是等于互联网领域是一个可以为所欲为的法外空间。竞争自由和创新自由必须以不侵犯他人合法权益为边界，互联网的健康发展需要有序的市场环境和明确的市场竞争规则作为保障。是否属于互联网精神鼓励的自由竞争和创新，仍然需要以是否有利于建立平等公平的竞争秩序、是否符合消费者的一般权益和社会公共利益为标准来进行判断，而不是仅有某些技术上的进步即应认为属于自由竞争和创新。否则，任何人均可以技术进步为借口，对他人的技术产品或者服务进行任意干涉，就将导致借技术进步、创新之名，而行“丛林法则”之实。技术本身虽然是中立的，但技术也可以成为进行不正当竞争的工具。技术革新应当成为公平自由竞争的工具，而非干涉他人正当商业模式的借口。360以技术创新为借口，专门开发扣扣保镖对QQ软件进行深度干预，不符合互联网自由和创新之精神。

五、消费者拥有自主选择权，市场竞争主体无权以为广大消费者利益为名对他人合法经营模式进行干预

最高人民法院在判决中指出：消费者的需求多种多样，不能简单地以某一或者部分消费者的感受和选择，特别是不能以360自己的标准来判断其他企业商业模式是否具有侵害性。消费者是相关消费体验的最佳判断者，在给予全面正确的信息后，相关消费者会自行对是否选用某种互联网产品作出判断；消费者能够接受经营者提供的某种产品或服务方式，也主要由市场需求和竞争状况进行调节；如果其不喜欢某种互联网产品的用户体验，也可以通过改用其他产品而“用脚投票”。因此，随着市场竞争的发展和消费者需求的提高，经营者必然会不断改进商业模式和提高服务质量。因此，360不能以自己的标准来认定QQ软件具有侵害性，从而主张其行为具有正当性。

对于360所提出的QQ涉及比较严重的捆绑和搭售问题，如果消费者

没有选择权和反制手段，消费者利益和整个互联网市场必将受到严重损害的问题。最高人民法院认为，QQ 是否构成捆绑和搭售，属于有关行政机关和司法机关依法认定的范畴，360 作为与腾讯平等的民事主体，无权以自己的标准对腾讯的行为作出评判并采取措施，无权以为广大消费者利益为名对被上诉人合法的经营模式等进行干预。

六、行业性规范是司法审判中发现和认定行业惯常行为和公认商业道德的重要渊源

近年来，行政主管部门和行业协会对互联网产业的竞争问题日益重视，出台了一系列规章和自律公约，例如，工业和信息化部出台了《规范互联网信息服务市场秩序若干规定》，互联网协会组织企业签署了《互联网终端软件服务行业自律公约》、《互联网搜索引擎服务自律公约》和《互联网终端安全服务自律公约》，这对这些行业性规范在司法审判中的价值，最高人民法院明确指出：这些行业性规范是结合行业特点和竞争需求，在总结归纳行业竞争现象的基础上所指定的行业内的从业规范，以约束行业内的企业行为或者为其提供行为指引，这些规范常常反映和体现了行业内的公认商业道德和行为标准，并且为业界广泛签署，其相关内容反映了互联网行业市场竞争的实际和正当竞争需求。人民法院在判断其内容合法、公正和客观的基础上，可以将其作为认定互联网行业惯常行为标准和公认商业道德的参考。

九、袁腾飞诉北京多看科技有限公司侵犯信息网络传播权纠纷案^①

法院审理认为，袁腾飞（原告）系涉案作品的著作权人，依法享有该书的信息网络传播权。多看网站（被告经营网站）上的涉案图书，包含了《历史 1》内容，未经袁腾飞许可，显然属于侵犯袁腾飞信息网

^① 参见北京市朝阳区人民法院民事判决书（2013）朝民初字第 03129 号。

络传播权的侵权作品。

本案中，多看科技公司在其所有的多看阅读软件上提供了侵权图书的下载服务，虽然多看科技公司辩称多看阅读软件仅仅是提供《历史 1》的网络搜索服务，但就此并未提交证据。从涉案公证书中看，多看阅读软件对涉案图书的搜索和下载，均在多看阅读软件内完成，并未显示有第三方的信息，对多看科技公司的上述答辩意见，法院不予采纳。此外，无论多看科技公司对涉案侵权图书是否属于搜索行为，从侵权责任承担上看，如果多看科技公司对涉案侵权的发生具有主观过错，也应当承担相应侵权责任。本案中，法院认为多看科技公司对涉案侵权行为的发生，主观上具有过错，理由如下：《历史 1》属于畅销书籍，多看科技公司有理由知道《历史 1》有明确的著作权归属；多看阅读软件的侵权图书下载页面中包含《历史 1》的封面、作者信息以及图书的内容介绍，这些内容说明多看科技公司可以接触到侵权图书，也应当认识到多看阅读软件中的涉案图书存在侵犯著作权的较大可能性。基于多看科技公司的主观过错，多看科技公司对涉案侵权图书的传播，应当承担侵权责任。

十、北京奇虎科技有限公司诉腾讯科技（深圳）有限公司等滥用市场支配地位纠纷案^①

法院审理认为：

一、关于相关市场如何界定的问题

相关商品市场，是根据商品的特性、用途及价格等因素，由需求者认为具有较为紧密替代关系的一组或一类商品所构成的市场。这些商品表现出较强的竞争关系，在反垄断执法中可以作为经营者进行竞争的商品范围。相关地域市场，是指需求者获取具有较为紧密替代关

^① 参加广东省高级人民法院民事判决书（2011）粤高法民三初字第 2 号。

系的商品的地理区域。这些地域表现出较强的竞争关系，在反垄断执法中可以作为经营者进行竞争的地域范围。

（一）相关商品市场

考虑到需求替代，消费者能够轻易、立刻、免费地在文字、音频和视频即时通信三种服务间转换；从供给替代出发，大部分服务商都能够同时提供该三种功能的服务。故不应当依据功能来区分文字即时通信、语音和视频通话，从而将该三种产品和服务分别视为独立的通信服务，而应当把它们作为更广阔市场的一部分；它们中的任何一种都不构成一个独立的市场，把即时通信市场分成更小的在功能上又没有重叠的市场是非常困难的。同时，本案证据显示消费者对即时通信产品及服务具有很高的价格敏感度，不愿意为使用即时通信的基础服务支出任何费用，如果被告持久地（假定为1年）从零价格改为小幅度收费的话，法院有理由相信需求者完全有可能转而选择免费的文字即时通信、音频或者视频通话中的任何一种服务，从而使被告的收费行为无利可图。综合性的即时通信与文字、音频以及视频等单一的即时通信之间具有紧密的可替代性，属于同一相关市场的商品集合。

（二）相关地域市场的界定

由于互联网的开放性和互通性，经营者和用户均无国界，本案证据显示境外经营者可向中国大陆地区用户提供即时通信服务，被告也同时向世界各地的用户提供服务。首先有一定数量的中国香港、澳门、台湾地区以及分布在世界各地的中文用户在使用被告提供的即时通信产品服务；同时也有分布在各国和地区的外文用户在使用被告提供的外文版本的即时通信服务。其次，用户的语言偏好和产品使用习惯不能作为划分地域市场的唯一依据。如前所述经营者通常都会提供多个语言版本的即时通信软件来满足不同语言需求的使用者。中国大陆用户经常会选择境外经营者提供的即时通信服务（例如MSN、ICQ、雅虎通、Skype等），用户语言偏好不会导致国外即时通信服务的经营者

无法与中国大陆经营者进行竞争。在产品使用习惯上,艾瑞咨询报告认为 TOM-Skype 提供了全球搜索目录,用户可以根据不同的查询条件查询认识的或者不认识的朋友,并且可以马上开始进行畅通无阻的语音聊天。在微软公司 /Skype 案中欧盟委员会认为,由于全球范围内的用户在接受即时通信服务方面的习惯是相同的,故不会导致用户因使用习惯差异带来经营者产品和服务的地域局限。再次,即时通信产品和服务的市场参与者在全球范围内提供和获得即时通信服务时,并无额外运输成本、价格成本或者其他成本。目前也尚未出现法律或技术上的标准来限制这些服务在全球范围内的提供和使用。综上所述,法院认为本案相关地域市场应为全球市场。

二、关于被告在相关市场上是否具有支配地位的问题

由于互联网行业特殊的市场状况,尤其不能将市场份额作为认定经营者市场支配地位的决定性因素,即使在原告所主张的最窄的相关市场内,正如 CNNIC 报告所述,腾讯的市场优势地位并未抑制和缩小其他即时通信产品的市场发展空间,亦不构成该市场整体发展的阻碍因素。腾讯在该市场不具有支配地位。

三、关于被告是否滥用市场支配地位,排除、限制竞争的问题

(一) 关于被告实施的“产品不兼容”行为(用户二选一)实质

在本案中,被告强迫用户“二选一”,表面上赋予用户选择权,但假如被告是一个具有市场支配地位的经营者的话,用户极有可能放弃 360 而选择 QQ。被告采取“二选一”的目的不是要拒绝与用户交易,而在于逼迫用户只能与其进行交易而不与 360 进行交易。被告该行为实质上仍然属于限制交易的行为。本案中,无论原告是否存在胁迫用户使用扣扣保镖的行为,是否劫持了 QQ 的安全模块并导致 QQ 失去相关功能,被告都无权逼迫用户对后者的 QQ 账户安全采取行动,被告的权利范围在于对此作出相应的风险提示,是否卸除 360 软件是用户

自身固有的权利，被告不能代替用户作出选择，强迫用户“二选一”的行为超出了必要的限度。

（二）被告是否存在《反垄断法》第十七条第一款第（五）项所禁止的无正当理由搭售的问题

根据反垄断法的规定，搭售是指具有支配地位的企业强迫交易对方购买从性质、交易习惯上均与合同无关的产品或服务的行为。搭售的目的是为了将市场支配地位扩大到被搭售产品的市场上，或者妨碍潜在的竞争者进入。构成搭售应当符合以下标准：搭售产品和被搭售产品是单独的产品；搭售者拥有市场支配地位；搭售者使消费者除了购买被搭售产品外别无选择；搭售是一种不合理的安排，即搭售不是出于该商品的交易习惯；若将搭售的商品分开销售，也不会有损于该商品的性能或使用价值；搭售具有反竞争效果。本案中被告 QQ 软件的主要功能是即时通信，与 QQ 医生、QQ 管家、安全管家、安全管理等一系列软件确属单独的软件产品；但第一，被告在即时通信市场中不具有市场支配地位。第二，被告没有限制用户的选择权。被告在 QQ 软件打包安装 QQ 软件管理时，为用户提供了 QQ 软件管理的卸载功能，被告向用户提供 QQ 软件服务并非以用户必须使用 QQ 软件管理为先决条件，对用户没有强制性；另外，被告在将 QQ 软件管理与 QQ 医生升级为 QQ 电脑管家时，向用户发出了升级公告，必须经过用户选择才可进行升级，已尽了明示用户并给予用户使用选择权的义务。第三，被告的相关行为具有经济合理性。QQ 软件管理与 QQ 软件的打包安装作为产品的功能整合，有利于用户通过使用辅助性工具软件更好地管理 QQ，保障用户 QQ 软件的账号安全；相反，若被告在提供 QQ 即时通信软件时不提供安全产品的，则可能会有损于 QQ 软件产品的性能或使用价值。第四，被告的相关行为未产生限制或排除竞争的效果。原告没有任何证据证明被告相关的打包安装行为导致了原告同类产品的市场占有率显著下降；也无证据证明该行为对同一市场内其他竞争

者产生了限制或排除竞争的后果。第五，原告没有提供证据证明被告QQ软件打包安装QQ软件管理以及QQ软件管理、QQ医生升级为QQ电脑管家的行为已经造成或者将会造成消费者的损害。因此，原告所诉被告实施了滥用市场支配地位的搭售行为不能成立。

附录



附录 A 国家层面立法摘编

1. 《全国人民代表大会常务委员会关于加强网络信息保护的決定》

一、国家保护能够识别公民个人身份和涉及公民个人隐私的电子
信息。

任何组织和个人不得窃取或者以其他非法方式获取公民个人电子
信息，不得出售或者非法向他人提供公民个人电子信息。

二、网络服务提供者和其他企业事业单位在业务活动中收集、使用
公民个人电子信息，应当遵循合法、正当、必要的原则，明示收集、使
用信息的目的、方式和范围，并经被收集者同意，不得违反法律、法规
的规定和双方的约定收集、使用信息。

网络服务提供者和其他企业事业单位收集、使用公民个人电子信
息，应当公开其收集、使用规则。

三、网络服务提供者和其他企业事业单位及其工作人员对在业务
活动中收集的公民个人电子信息必须严格保密，不得泄露、篡改、毁损，
不得出售或者非法向他人提供。

四、网络服务提供者和其他企业事业单位应当采取技术措施和其
他必要措施，确保信息安全，防止在业务活动中收集的公民个人电子
信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失
的情况时，应当立即采取补救措施。

五、网络服务提供者应当加强对其用户发布的信息的管理，发现

法律、法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

六、网络服务提供者为用户办理网站接入服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布服务，应当在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息。

七、任何组织和个人未经电子信息接收者同意或者请求，或者电子信息接收者明确表示拒绝的，不得向其固定电话、移动电话或者个人电子邮箱发送商业性电子信息。

八、公民发现泄露个人身份、散布个人隐私等侵害其合法权益的网络信息，或者受到商业性电子信息侵扰的，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止。

九、任何组织和个人对窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为，有权向有关主管部门举报、控告；接到举报、控告的部门应当依法及时处理。被侵权人可以依法提起诉讼。

十、有关主管部门应当在各自职权范围内依法履行职责，采取技术措施和其他必要措施，防范、制止和查处窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为。有关主管部门依法履行职责时，网络服务提供者应当予以配合，提供技术支持。

国家机关及其工作人员对在履行职责中知悉的公民个人电子信息应当予以保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

十一、对有违反本决定行为的，依法给予警告、罚款、没收违法所得、吊销许可证或者取消备案、关闭网站、禁止有关责任人员从事网络服务业务等处罚，记入社会信用档案并予以公布；构成违反治安管理行为的，依法给予治安管理处罚。构成犯罪的，依法追究刑事责任。

侵害他人民事权益的，依法承担民事责任。

十二、本决定自公布之日起施行。

2. 《电信和互联网用户个人信息保护规定》

第一章 总 则

第一条 为了保护电信和互联网用户的合法权益，维护网络信息安全，根据《全国人民代表大会常务委员会关于加强网络信息保护的決定》、《中华人民共和国电信条例》和《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 在中华人民共和国境内提供电信服务和互联网信息服务过程中收集、使用用户个人信息的活动，适用本规定。

第三条 工业和信息化部 and 各省、自治区、直辖市通信管理局（以下统称电信管理机构）依法对电信和互联网用户个人信息保护工作实施监督管理。

第四条 本规定所称用户个人信息，是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。

第五条 电信业务经营者、互联网信息服务提供者在提供服务的过程中收集、使用用户个人信息，应当遵循合法、正当、必要的原则。

第六条 电信业务经营者、互联网信息服务提供者对其在提供服务过程中收集、使用的用户个人信息的安全负责。

第七条 国家鼓励电信和互联网行业开展用户个人信息保护自律工作。

第二章 信息收集和使用规范

第八条 电信业务经营者、互联网信息服务提供者应当制定用户个人信息收集、使用规则，并在其经营或者服务场所、网站等予以公布。

第九条 未经用户同意，电信业务经营者、互联网信息服务提供者不得收集、使用用户个人信息。

电信业务经营者、互联网信息服务提供者收集、使用用户个人信息的，应当明确告知用户收集、使用信息的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果等事项。

电信业务经营者、互联网信息服务提供者不得收集其提供服务所必需以外的用户个人信息或者将信息用于提供服务之外的目的，不得以欺骗、误导或者强迫等方式或者违反法律、行政法规以及双方的约定收集、使用信息。

电信业务经营者、互联网信息服务提供者在用户终止使用电信服务或者互联网信息服务后，应当停止对用户个人信息的收集和使用，并为用户提供注销号码或者账号的服务。

法律、行政法规对本条第一款至第四款规定的情形另有规定的，从其规定。

第十条 电信业务经营者、互联网信息服务提供者及其工作人员对在提供服务过程中收集、使用的用户个人信息应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第十一条 电信业务经营者、互联网信息服务提供者委托他人代理市场销售和技术服务等直接面向用户的服务性工作，涉及收集、使用用户个人信息的，应当对代理人的用户个人信息保护工作进行监督和管理，不得委托不符合本规定有关用户个人信息保护要求的代理人代办相关服务。

第十二条 电信业务经营者、互联网信息服务提供者应当建立用户投诉处理机制，公布有效的联系方式，接受与用户个人信息保护有关的投诉，并自接到投诉之日起十五日内答复投诉人。

第三章 安全保障措施

第十三条 电信业务经营者、互联网信息服务提供者应当采取以下措施防止用户个人信息泄露、毁损、篡改或者丢失：

（一）确定各部门、岗位和分支机构的用户个人信息安全管理责任；

（二）建立用户个人信息收集、使用及其相关活动的工作流程和安全管理制

度；

（三）对工作人员及代理人实行权限管理，对批量导出、复制、销毁信息实行审查，并采取防泄密措施；

（四）妥善保管记录用户个人信息的纸介质、光介质、电磁介质等载体，并采取相应的安全储存措施；

（五）对储存用户个人信息的信息系统实行接入审查，并采取防入侵、防病毒等措施；

（六）记录对用户个人信息进行操作的人员、时间、地点、事项等信息；

（七）按照电信管理机构的规定开展通信网络安全防护工作；

（八）电信管理机构规定的其他必要措施。

第十四条 电信业务经营者、互联网信息服务提供者保管的用户个人信息发生或者可能发生泄露、毁损、丢失的，应当立即采取补救措施；造成或者可能造成严重后果的，应当立即向准予其许可或者备案的电信管理机构报告，配合相关部门进行调查处理。

电信管理机构应当对报告或者发现的可能违反本规定行为的影响

进行评估；影响特别重大的，相关省、自治区、直辖市通信管理局应当向工业和信息化部报告。电信管理机构在依据本规定作出处理决定前，可以要求电信业务经营者和互联网信息服务提供者暂停有关行为，电信业务经营者和互联网信息服务提供者应当执行。

第十五条 电信业务经营者、互联网信息服务提供者应当对其工作人员进行用户个人信息保护相关知识、技能和安全责任培训。

第十六条 电信业务经营者、互联网信息服务提供者应当对用户个人信息保护情况每年至少进行一次自查，记录自查情况，及时消除自查中发现的安全隐患。

第四章 监督检查

第十七条 电信管理机构应当对电信业务经营者、互联网信息服务提供者保护用户个人信息的情况实施监督检查。

电信管理机构实施监督检查时，可以要求电信业务经营者、互联网信息服务提供者提供相关材料，进入其生产经营场所调查情况，电信业务经营者、互联网信息服务提供者应当予以配合。

电信管理机构实施监督检查，应当记录监督检查的情况，不得妨碍电信业务经营者、互联网信息服务提供者正常的经营或者服务活动，不得收取任何费用。

第十八条 电信管理机构及其工作人员对在履行职责中知悉的用户个人信息应当予以保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供。

第十九条 电信管理机构实施电信业务经营许可及经营许可证年检时，应当对用户个人信息保护情况进行审查。

第二十条 电信管理机构应当将电信业务经营者、互联网信息服务提供者违反本规定的行为记入其社会信用档案并予以公布。

第二十一条 鼓励电信和互联网行业协会依法制定有关用户个人信息保护的自律性管理制度，引导会员加强自律管理，提高用户个人信息保护水平。

第五章 法律责任

第二十二条 电信业务经营者、互联网信息服务提供者违反本规定第八条、第十二条规定的，由电信管理机构依据职权责令限期改正，予以警告，可以并处一万元以下的罚款。

第二十三条 电信业务经营者、互联网信息服务提供者违反本规定第九条至第十一条、第十三条至第十六条、第十七条第二款规定的，由电信管理机构依据职权责令限期改正，予以警告，可以并处一万元以上三万元以下的罚款，向社会公告；构成犯罪的，依法追究刑事责任。

第二十四条 电信管理机构工作人员在对用户个人信息保护工作实施监督管理的过程中玩忽职守、滥用职权、徇私舞弊的，依法给予处理；构成犯罪的，依法追究刑事责任。

第六章 附 则

第二十五条 本规定自 2013 年 9 月 1 日起施行。

3. 《中华人民共和国消费者权益保护法》（2013 年修正）

（涉及电子商务方面）

第二十五条 经营者采用网络、电视、电话、邮购等方式销售商品，消费者有权自收到商品之日起七日内退货，且无须说明理由，但下列商品除外：

（一）消费者定做的；

（二）鲜活易腐的；

（三）在线下载或者消费者拆封的音像制品、计算机软件等数字化商品；

（四）交付的报纸、期刊。

除前款所列商品外，其他根据商品性质并经消费者在购买时确认不宜退货的商品，不适用无理由退货。

消费者退货的商品应当完好。经营者应当自收到退回商品之日起七日内返还消费者支付的商品价款。退回商品的运费由消费者承担；经营者和消费者另有约定的，按照约定。

第四十四条 消费者通过网络交易平台购买商品或者接受服务，其合法权益受到损害的，可以向销售者或者服务者要求赔偿。网络交易平台提供者不能提供销售者或者服务者的真实名称、地址和有效联系方式的，消费者也可以向网络交易平台提供者要求赔偿；网络交易平台提供者作出更有利于消费者的承诺的，应当履行承诺。网络交易平台提供者赔偿后，有权向销售者或者服务者追偿。

网络交易平台提供者明知或者应知销售者或者服务者利用其平台侵害消费者合法权益，未采取必要措施的，依法与该销售者或者服务者承担连带责任。

4. 《网络发票管理办法》

第一条 为加强普通发票管理，保障国家税收收入，规范网络发票的开具和使用，根据《中华人民共和国发票管理办法》规定，制定本办法。

第二条 在中华人民共和国境内使用网络发票管理系统开具发票的单位和个人办理网络发票管理系统的开户登记、网上领取发票手续、在线开具、传输、查验和缴销等事项，适用本办法。

第三条 本办法所称网络发票是指符合国家税务总局统一标准并通过国家税务总局及省、自治区、直辖市国家税务局、地方税务局公布的网络发票管理系统开具的发票。

国家积极推广使用网络发票管理系统开具发票。

第四条 税务机关应加强网络发票的管理,确保网络发票的安全、唯一、便利,并提供便捷的发票信息查询渠道;应通过应用网络发票数据分析,提高信息管税水平。

第五条 税务机关应根据开具发票的单位和个人的经营情况,核定其在线开具网络发票的种类、行业类别、开票限额等内容。

开具发票的单位和个人需要变更网络发票核定内容的,可向税务机关提出书面申请,经税务机关确认,予以变更。

第六条 开具发票的单位和个人开具网络发票应登录网络发票管理系统,如实完整填写发票的相关内容,确认保存后打印发票。

开具发票的单位和个人在线开具的网络发票,经系统自动保存数据后即完成开票信息的确认、查验。

第七条 单位和个人取得网络发票时,应及时查询验证网络发票信息的真实性、完整性,对不符合规定的发票,不得作为财务报销凭证,任何单位和个人有权拒收。

第八条 开具发票的单位和个人需要开具红字发票的,必须收回原网络发票全部联次或取得受票方出具的有效证明,通过网络发票管理系统开具金额为负数的红字网络发票。

第九条 开具发票的单位和个人作废开具的网络发票,应收回原网络发票全部联次,注明“作废”,并在网络发票管理系统中进行发票作废处理。

第十条 开具发票的单位和个人应当在办理变更或者注销税务登

记的同时，办理网络发票管理系统的用户变更、注销手续并缴销空白发票。

第十一条 税务机关根据发票管理的需要，可以按照国家税务总局的规定委托其他单位通过网络发票管理系统代开网络发票。

税务机关应当与受托代开发票的单位签订协议，明确代开网络发票的种类、对象、内容和相关责任等内容。

第十二条 开具发票的单位和个人必须如实在线开具网络发票，不得利用网络发票进行转借、转让、虚开发票及其他违法活动。

第十三条 开具发票的单位和个人在网络出现故障，无法在线开具发票时，可离线开具发票。

开具发票后，不得改动开票信息，并于 48 小时内上传开票信息。

第十四条 开具发票的单位和个人违反本办法规定的，按照《中华人民共和国发票管理办法》有关规定处理。

第十五条 省以上税务机关在确保网络发票电子信息正确生成、可靠存储、查询验证、安全唯一等条件的情况下，可以试行电子发票。

第十六条 本办法自 2013 年 4 月 1 日起施行。

5. 《规范互联网信息服务市场秩序若干规定》

第一条 为了规范互联网信息服务市场秩序，保护互联网信息服务提供者和用户的合法权益，促进互联网行业的健康发展，根据《中华人民共和国电信条例》、《互联网信息服务管理办法》等法律、行政法规的规定，制定本规定。

第二条 在中华人民共和国境内从事互联网信息服务及与互联网信息服务有关的活动，应当遵守本规定。

第三条 工业和信息化部 and 各省、自治区、直辖市通信管理局（以下统称“电信管理机构”）依法对互联网信息服务活动实施监督管理。

第四条 互联网信息服务提供者应当遵循平等、自愿、公平、诚信的原则提供服务。

第五条 互联网信息服务提供者不得实施下列侵犯其他互联网信息服务提供者合法权益的行为：

（一）恶意干扰用户终端上其他互联网信息服务提供者的服务，或者恶意干扰与互联网信息服务相关的软件等产品（“与互联网信息服务相关的软件等产品”，以下简称“产品”）的下载、安装、运行和升级；

（二）捏造、散布虚假事实损害其他互联网信息服务提供者的合法权益，或者诋毁其他互联网信息服务提供者的服务或者产品；

（三）恶意对其他互联网信息服务提供者的服务或者产品实施不兼容；

（四）欺骗、误导或者强迫用户使用或者不使用其他互联网信息服务提供者的服务或者产品；

（五）恶意修改或者欺骗、误导、强迫用户修改其他互联网信息服务提供者的服务或者产品参数；

（六）其他违反国家法律规定，侵犯其他互联网信息服务提供者合法权益的行为。

第六条 对互联网信息服务提供者的服务或者产品进行评测，应当客观公正。

评测方公开或者向用户提供评测结果的，应当同时提供评测实施者、评测方法、数据来源、用户原始评价、评测手段和评测环境等与评测活动相关的信息。评测结果应当真实准确，与评测活动相关的信息应当完

整全面。被评测的服务或者产品与评测方的服务或者产品相同或者功能类似的，评测结果中不得含有评测方的主观评价。

被评测方对评测结果有异议的，可以自行或者委托第三方就评测结果进行再评测，评测方应当予以配合。

评测方不得利用评测结果，欺骗、误导、强迫用户对被评测方的服务或者产品作出处置。

本规定所称评测，是指提供平台供用户评价，或者以其他方式对互联网信息服务或者产品的性能等进行评价和测试。

第七条 互联网信息服务提供者不得实施下列侵犯用户合法权益的行为：

（一）无正当理由拒绝、拖延或者中止向用户提供互联网信息服务或者产品；

（二）无正当理由限定用户使用或者不使用其指定的互联网信息服务或者产品；

（三）以欺骗、误导或者强迫等方式向用户提供互联网信息服务或者产品；

（四）提供的互联网信息服务或者产品与其向用户所作的宣传或者承诺不符；

（五）擅自改变服务协议或者业务规程，降低服务质量或者加重用户责任；

（六）与其他互联网信息服务提供者的服务或者产品不兼容时，未主动向用户提示和说明；

（七）未经提示并由用户主动选择同意，修改用户浏览器配置或者其他设置；

（八）其他违反国家法律规定，侵犯用户合法权益的行为。

第八条 互联网信息服务提供者在用户终端上进行软件下载、安装、运行、升级、卸载等操作的，应当提供明确、完整的软件功能等信息，并事先征得用户同意。

互联网信息服务提供者不得实施下列行为：

（一）欺骗、误导或者强迫用户下载、安装、运行、升级、卸载软件；

（二）未提供与软件安装方式同等或者更便捷的卸载方式；

（三）在未受其他软件影响和人为破坏的情况下，未经用户主动选择同意，软件卸载后有可执行代码或者其他不必要的文件驻留在用户终端。

第九条 互联网信息服务终端软件捆绑其他软件的，应当以显著的方式提示用户，由用户主动选择是否安装或者使用，并提供独立的卸载或者关闭方式，不得附加不合理条件。

第十条 互联网信息服务提供者在用户终端弹出广告或者其他与终端软件功能无关的信息窗口的，应当以显著的方式向用户提供关闭或者退出窗口的功能标识。

第十一条 未经用户同意，互联网信息服务提供者不得收集与用户相关、能够单独或者与其他信息结合识别用户的信息（以下简称“用户个人信息”），不得将用户个人信息提供给他人，但是法律、行政法规另有规定的除外。

互联网信息服务提供者经用户同意收集用户个人信息的，应当明确告知用户收集和处理用户个人信息的方式、内容和用途，不得收集其提供服务所必须以外的信息，不得将用户个人信息用于其提供服务之外的目的。

第十二条 互联网信息服务提供者应当妥善保管用户个人信息；

保管的用户个人信息泄露或者可能泄露时，应当立即采取补救措施；造成或者可能造成严重后果的，应当立即向准予其互联网信息服务许可或者备案的电信管理机构报告，并配合相关部门进行的调查处理。

第十三条 互联网信息服务提供者应当加强系统安全防护，依法维护用户上载信息的安全，保障用户对上载信息的使用、修改和删除。

互联网信息服务提供者不得有下列行为：

（一）无正当理由擅自修改或者删除用户上载信息；

（二）未经用户同意，向他人提供用户上载信息，但是法律、行政法规另有规定的除外；

（三）擅自或者假借用户名义转移用户上载信息，或者欺骗、误导、强迫用户转移其上载信息；

（四）其他危害用户上载信息安全的行为。

第十四条 互联网信息服务提供者应当以显著的方式公布有效联系方式，接受用户及其他互联网信息服务提供者的投诉，并自接到投诉之日起十五日内作出答复。

第十五条 互联网信息服务提供者认为其他互联网信息服务提供者实施违反本规定的行为，侵犯其合法权益并对用户权益造成或者可能造成重大影响的，应当立即向准予该其他互联网信息服务提供者互联网信息服务许可或者备案的电信管理机构报告。

电信管理机构应当对报告或者发现的可能违反本规定的行为的影响进行评估；影响特别重大的，相关省、自治区、直辖市通信管理局应当向工业和信息化部报告。电信管理机构在依据本规定作出处理决定前，可以要求互联网信息服务提供者暂停有关行为，互联网信息服务提供者应当执行。

第十六条 互联网信息服务提供者违反本规定第五条、第七条或者第十三条规定的，由电信管理机构依据职权责令改正，处以警告，可以并处一万元以上三万元以下的罚款，向社会公告；其中，《中华人民共和国电信条例》或者《互联网信息服务管理办法》规定法律责任的，依照其规定处理。

第十七条 评测方违反本规定第六条规定的，由电信管理机构依据职权处以警告，可以并处一万元以上三万元以下的罚款，向社会公告。

第十八条 互联网信息服务提供者违反本规定第八条、第九条、第十条、第十一条、第十二条或者第十四条规定的，由电信管理机构依据职权处以警告，可以并处一万元以上三万元以下的罚款，向社会公告。

第十九条 互联网信息服务提供者违反本规定第十五条规定的，不执行电信管理机构暂停有关行为的要求的，由电信管理机构依据职权处以警告，向社会公告。

第二十条 互联网信息服务提供者违反其他法律、行政法规规定的，依照其规定处理。

第二十一条 本规定自 2012 年 3 月 15 日起施行。

6. 《国务院关于修改〈中华人民共和国计算机软件保护条例〉的决定》

国务院决定对《计算机软件保护条例》作如下修改：

将第二十四条第二款修改为：“有前款第一项或者第二项行为的，可以并处每件 100 元或者货值金额 1 倍以上 5 倍以下的罚款；有前款第三项、第四项或者第五项行为的，可以并处 20 万元以下的罚款。”

本决定自 2013 年 3 月 1 日起施行。《计算机软件保护条例》根据本决定作相应修改，重新公布。

中华人民共和国计算机软件保护条例

（2001 年 12 月 20 日中华人民共和国国务院令第 339 号公布，根据 2011 年 1 月 8 日《国务院关于废止和修改部分行政法规的决定》第一次修订，根据 2013 年 1 月 30 日《国务院关于修改〈计算机软件保护条例〉的决定》第二次修订）

第一章 总 则

第一条 为了保护计算机软件著作权人的权益，调整计算机软件在开发、传播和使用中发生的利益关系，鼓励计算机软件的开发与应用，促进软件产业和国民经济信息化的发展，根据《中华人民共和国著作权法》，制定本条例。

第二条 本条例所称计算机软件（以下简称软件），是指计算机程序及其有关文档。

第三条 本条例下列用语的含义：

（一）计算机程序，是指为了得到某种结果而可以由计算机等具有信息处理能力的装置执行的代码化指令序列，或者可以被自动转换成代码化指令序列的符号化指令序列或者符号化语句序列。同一计算机程序的源程序和目标程序为同一作品。

（二）文档，是指用来描述程序的内容、组成、设计、功能规格、开发情况、测试结果及使用方法文字资料和图表等，如程序设计说明书、流程图、用户手册等。

（三）软件开发，是指实际组织开发、直接进行开发，并对开发完成的软件承担责任的法人或者其他组织；或者依靠自己具有的条

件独立完成软件开发，并对软件承担责任的自然人。

（四）软件著作权人，是指依照本条例的规定，对软件享有著作权的自然人、法人或者其他组织。

第四条 受本条例保护的软件必须由开发者独立开发，并已固定在某种有形物体上。

第五条 中国公民、法人或者其他组织对其所开发的软件，不论是否发表，依照本条例享有著作权。

外国人、无国籍人的软件首先在中国境内发行的，依照本条例享有著作权。

外国人、无国籍人的软件，依照其开发者所属国或者经常居住地国同中国签订的协议或者依照中国参加的国际条约享有的著作权，受本条例保护。

第六条 本条例对软件著作权的保护不延及开发软件所用的思想、处理过程、操作方法或者数学概念等。

第七条 软件著作权人可以向国务院著作权行政管理部门认定的软件登记机构办理登记。软件登记机构发放的登记证明文件是登记事项的初步证明。

办理软件登记应当缴纳费用。软件登记的收费标准由国务院著作权行政管理部门会同国务院价格主管部门规定。

第二章 软件著作权

第八条 软件著作权人享有下列各项权利：

- （一）发表权，即决定软件是否公之于众的权利；
- （二）署名权，即表明开发者身份，在软件上署名的权利；

（三）修改权，即对软件进行增补、删节，或者改变指令、语句顺序的权利；

（四）复制权，即将软件制作一份或者多份的权利；

（五）发行权，即以出售或者赠与方式向公众提供软件的原件或者复制件的权利；

（六）出租权，即有偿许可他人临时使用软件的权利，但是软件不是出租的主要标的的除外；

（七）信息网络传播权，即以有线或者无线方式向公众提供软件，使公众可以在其个人选定的时间和地点获得软件的权利；

（八）翻译权，即将原软件从一种自然语言文字转换成另一种自然语言文字的权利；

（九）应当由软件著作权人享有的其他权利。

软件著作权人可以许可他人行使其软件著作权，并有权获得报酬。

软件著作权人可以全部或者部分转让其软件著作权，并有权获得报酬。

第九条 软件著作权属于软件开发者，本条例另有规定的除外。

如无相反证明，在软件上署名的自然人、法人或者其他组织为开发者。

第十条 由两个以上的自然人、法人或者其他组织合作开发的软件，其著作权的归属由合作开发者签订书面合同约定。无书面合同或者合同未作明确约定，合作开发的软件可以分割使用的，开发者对各自开发的部分可以单独享有著作权；但是，行使著作权时，不得扩展到合作开发的软件整体的著作权。合作开发的软件不能分割使用的，其著作权由各合作开发者共同享有，通过协商一致行使；不能协商一致，又无正当理由的，任何一方不得阻止他方行使除转让权以外的其他权利，但是所得

收益应当合理分配给所有合作开发者。

第十一条 接受他人委托开发的软件，其著作权的归属由委托人与受托人签订书面合同约定；无书面合同或者合同未作明确约定的，其著作权由受托人享有。

第十二条 由国家机关下达任务开发的软件，著作权的归属与行使由项目任务书或者合同规定；项目任务书或者合同中未作明确规定的，软件著作权由接受任务的法人或者其他组织享有。

第十三条 自然人在法人或者其他组织中任职期间所开发的软件有下列情形之一的，该软件著作权由该法人或者其他组织享有，该法人或者其他组织可以对开发软件的自然人进行奖励：

（一）针对本职工作中明确指定的开发目标所开发的软件；

（二）开发的软件是从事本职工作活动所预见的结果或者自然的结果；

（三）主要使用了法人或者其他组织的资金、专用设备、未公开的专门信息等物质技术条件所开发并由法人或者其他组织承担责任的软件。

第十四条 软件著作权自软件开发完成之日起产生。

自然人的软件著作权，保护期为自然人终生及其死亡后 50 年，截止于自然人死亡后第 50 年的 12 月 31 日；软件是合作开发的，截止于最后死亡的自然人死亡后第 50 年的 12 月 31 日。

法人或者其他组织的软件著作权，保护期为 50 年，截止于软件首次发表后第 50 年的 12 月 31 日，但软件自开发完成之日起 50 年内未发表的，本条例不再保护。

第十五条 软件著作权属于自然人的，该自然人死亡后，在软件著作权的保护期内，软件著作权的继承人可以依照《中华人民共和国

继承法》的有关规定，继承本条例第八条规定的除署名权以外的其他权利。

软件著作权属于法人或者其他组织的，法人或者其他组织变更、终止后，其著作权在本条例规定的保护期内由承受其权利义务的法人或者其他组织享有；没有承受其权利义务的法人或者其他组织的，由国家享有。

第十六条 软件的合法复制品所有人享有下列权利：

（一）根据使用的需要把该软件装入计算机等具有信息处理能力的装置内；

（二）为了防止复制品损坏而制作备份复制品。这些备份复制品不得通过任何方式提供给他人使用，并在所有人丧失该合法复制品的所有权时，负责将备份复制品销毁；

（三）为了把该软件用于实际的计算机应用环境或者改进其功能、性能而进行必要的修改；但是，除合同另有约定外，未经该软件著作权人许可，不得向任何第三方提供修改后的软件。

第十七条 为了学习和研究软件内含的设计思想和原理，通过安装、显示、传输或者存储软件等方式使用软件的，可以不经软件著作权人许可，不向其支付报酬。

第三章 软件著作权的许可使用和转让

第十八条 许可他人行使软件著作权的，应当订立许可使用合同。

许可使用合同中软件著作权人未明确许可的权利，被许可人不得行使。

第十九条 许可他人专有行使软件著作权的，当事人应当订立书面合同。

没有订立书面合同或者合同中未明确约定为专有许可的，被许可行使的权利应当视为非专有权利。

第二十条 转让软件著作权的，当事人应当订立书面合同。

第二十一条 订立许可他人专有行使软件著作权的许可合同，或者订立转让软件著作权合同，可以向国务院著作权行政管理部门认定的软件登记机构登记。

第二十二条 中国公民、法人或者其他组织向外国人许可或者转让软件著作权的，应当遵守《中华人民共和国技术进出口管理条例》的有关规定。

第四章 法律责任

第二十三条 除《中华人民共和国著作权法》或者本条例另有规定外，有下列侵权行为的，应当根据情况，承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任：

- （一）未经软件著作权人许可，发表或者登记其软件的；
- （二）将他人软件作为自己的软件发表或者登记的；
- （三）未经合作者许可，将与他人合作开发的软件作为自己单独完成的软件发表或者登记的；
- （四）在他人软件上署名或者更改他人软件上的署名的；
- （五）未经软件著作权人许可，修改、翻译其软件的；
- （六）其他侵犯软件著作权的行为。

第二十四条 除《中华人民共和国著作权法》、本条例或者其他法律、行政法规另有规定外，未经软件著作权人许可，有下列侵权行为的，应当根据情况，承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任；同时损害社会公共利益的，由著作权行政管理部门责

令停止侵权行为，没收违法所得，没收、销毁侵权复制品，可以并处罚款；情节严重的，著作权行政管理部门并可以没收主要用于制作侵权复制品的材料、工具、设备等；触犯刑律的，依照刑法关于侵犯著作权罪、销售侵权复制品罪的规定，依法追究刑事责任：

（一）复制或者部分复制著作权人的软件的；

（二）向公众发行、出租、通过信息网络传播著作权人的软件的；

（三）故意避开或者破坏著作权人为保护其软件著作权而采取的技术措施的；

（四）故意删除或者改变软件权利管理电子信息的；

（五）转让或者许可他人行使著作权人的软件著作权的。

有前款第一项或者第二项行为的，可以并处每件 100 元或者货值金额 1 倍以上 5 倍以下的罚款；有前款第三项、第四项或者第五项行为的，可以并处 20 万元以下的罚款。

第二十五条 侵犯软件著作权的赔偿数额，依照《中华人民共和国著作权法》第四十九条的规定确定。

第二十六条 软件著作权人有证据证明他人正在实施或者即将实施侵犯其权利的行为，如不及时制止，将会使其合法权益受到难以弥补的损害的，可以依照《中华人民共和国著作权法》第五十条的规定，在提起诉讼前向人民法院申请采取责令停止有关行为和财产保全的措施。

第二十七条 为了制止侵权行为，在证据可能灭失或者以后难以取得的情况下，软件著作权人可以依照《中华人民共和国著作权法》第五十一条的规定，在提起诉讼前向人民法院申请保全证据。

第二十八条 软件复制品的出版者、制作者不能证明其出版、制作有合法授权的，或者软件复制品的发行者、出租者不能证明其发行、出租的复制品有合法来源的，应当承担法律责任。

第二十九条 软件开发者的软件，由于可供选用的表达方式有限而与已经存在的软件相似的，不构成对已经存在的软件的著作权的侵犯。

第三十条 软件的复制品持有人不知道也没有合理理由应当知道该软件是侵权复制品的，不承担赔偿责任；但是，应当停止使用、销毁该侵权复制品。如果停止使用并销毁该侵权复制品将给复制品使用人造成重大损失的，复制品使用人可以在向软件著作权人支付合理费用后继续使用。

第三十一条 软件著作权侵权纠纷可以调解。

软件著作权合同纠纷可以依据合同中的仲裁条款或者事后达成的书面仲裁协议，向仲裁机构申请仲裁。

当事人没有在合同中订立仲裁条款，事后又没有书面仲裁协议的，可以直接向人民法院提起诉讼。

第五章 附 则

第三十二条 本条例施行前发生的侵权行为，依照侵权行为发生时的国家有关规定处理。

第三十三条 本条例自 2002 年 1 月 1 日起施行。1991 年 6 月 4 日国务院发布的《计算机软件保护条例》同时废止。

7. 《国务院关于修改〈中华人民共和国著作权法实施条例〉的决定》

国务院决定对《中华人民共和国著作权法实施条例》作如下修改：

将第三十六条修改为：“有著作权法第四十八条所列侵权行为，同时损害社会公共利益，非法经营额 5 万元以上的，著作权行政管理部门可处非法经营额 1 倍以上 5 倍以下的罚款；没有非法经营额或者

非法经营额 5 万元以下的，著作权行政管理部门根据情节轻重，可处 25 万元以下的罚款。”

本决定自 2013 年 3 月 1 日起施行。

《中华人民共和国著作权法实施条例》根据本决定作相应修改，重新公布。

中华人民共和国著作权法实施条例

（2002 年 8 月 2 日中华人民共和国国务院令 第 359 号公布，根据 2011 年 1 月 8 日《国务院关于废止和修改部分行政法规的决定》第一次修订，根据 2013 年 1 月 30 日《国务院关于修改〈中华人民共和国著作权法实施条例〉的决定》第二次修订）

第一条 根据《中华人民共和国著作权法》（以下简称著作权法），制定本条例。

第二条 著作权法所称作品，是指文学、艺术和科学领域内具有独创性并能以某种有形形式复制的智力成果。

第三条 著作权法所称创作，是指直接产生文学、艺术和科学作品的智力活动。

为他人创作进行组织工作，提供咨询意见、物质条件，或者其他辅助工作，均不视为创作。

第四条 著作权法和本条例中下列作品的含义：

（一）文字作品，是指小说、诗词、散文、论文等以文字形式表现的作品；

（二）口述作品，是指即兴的演说、授课、法庭辩论等以口头语言形式表现的作品；

（三）音乐作品，是指歌曲、交响乐等能够演唱或者演奏的带词或者不带词的作品；

（四）戏剧作品，是指话剧、歌剧、地方戏等供舞台演出的作品；

（五）曲艺作品，是指相声、快书、大鼓、评书等以说唱为主要形式表演的作品；

（六）舞蹈作品，是指通过连续的动作、姿势、表情等表现思想情感的作品；

（七）杂技艺术作品，是指杂技、魔术、马戏等通过形体动作和技巧表现的作品；

（八）美术作品，是指绘画、书法、雕塑等以线条、色彩或者其他方式构成的有审美意义的平面或者立体的造型艺术作品；

（九）建筑作品，是指以建筑物或者构筑物形式表现的有审美意义的作品；

（十）摄影作品，是指借助器械在感光材料或者其他介质上记录客观物体形象的艺术作品；

（十一）电影作品和以类似摄制电影的方法创作的作品，是指摄制在一定介质上，由一系列有伴音或者无伴音的画面组成，并且借助适当装置放映或者以其他方式传播的作品；

（十二）图形作品，是指为施工、生产绘制的工程设计图、产品设计图，以及反映地理现象、说明事物原理或者结构的地图、示意图等作品；

（十三）模型作品，是指为展示、试验或者观测等用途，根据物体的形状和结构，按照一定比例制成的立体作品。

第五条 著作权法和本条例中下列用语的含义：

（一）时事新闻，是指通过报纸、期刊、广播电台、电视台等媒体报道的单纯事实消息；

（二）录音制品，是指任何对表演的声音和其他声音的录制品；

（三）录像制品，是指电影作品和以类似摄制电影的方法创作的作品以外的任何有伴音或者无伴音的连续相关形象、图像的录制品；

（四）录音制作者，是指录音制品的首次制作人；

（五）录像制作者，是指录像制品的首次制作人；

（六）表演者，是指演员、演出单位或者其他表演文学、艺术作品的人。

第六条 著作权自作品创作完成之日起产生。

第七条 著作权法第二条第三款规定的首先在中国境内出版的外国人、无国籍人的作品，其著作权自首次出版之日起受保护。

第八条 外国人、无国籍人的作品在中国境外首先出版后，30日内在中国境内出版的，视为该作品同时在中国境内出版。

第九条 合作作品不可以分割使用的，其著作权由各合作作者共同享有，通过协商一致行使；不能协商一致，又无正当理由的，任何一方不得阻止他方行使除转让以外的其他权利，但是所得收益应当合理分配给所有合作作者。

第十条 著作权人许可他人将其作品摄制成电影作品和以类似摄制电影的方法创作的作品的，视为已同意对其作品进行必要的改动，但是这种改动不得歪曲篡改原作品。

第十一条 著作权法第十六条第一款关于职务作品的规定中的“工作任务”，是指公民在该法人或者该组织中应当履行的职责。

著作权法第十六条第二款关于职务作品的规定中的“物质技术条

件”，是指该法人或者该组织为公民完成创作专门提供的资金、设备或者资料。

第十二条 职务作品完成两年内，经单位同意，作者许可第三人以与单位使用的相同方式使用作品所获报酬，由作者与单位按约定的比例分配。

作品完成两年的期限，自作者向单位交付作品之日起计算。

第十三条 作者身份不明的作品，由作品原件的所有人行使除署名权以外的著作权。作者身份确定后，由作者或者其继承人行使著作权。

第十四条 合作作者之一死亡后，其对合作作品享有的著作权法第十条第一款第五项至第十七项规定的权利无人继承又无人受遗赠的，由其他合作作者享有。

第十五条 作者死亡后，其著作权中的署名权、修改权和保护作品完整权由作者的继承人或者受遗赠人保护。

著作权无人继承又无人受遗赠的，其署名权、修改权和保护作品完整权由著作权行政管理部门保护。

第十六条 国家享有著作权的作品的使用，由国务院著作权行政管理部门管理。

第十七条 作者生前未发表的作品，如果作者未明确表示不发表，作者死亡后 50 年内，其发表权可由继承人或者受遗赠人行使；没有继承人又无人受遗赠的，由作品原件的所有人行使。

第十八条 作者身份不明的作品，其著作权法第十条第一款第五项至第十七项规定的权利的保护期截止于作品首次发表后第 50 年的 12 月 31 日。作者身份确定后，适用著作权法第二十一条的规定。

第十九条 使用他人作品的，应当指明作者姓名、作品名称；但是，当事人另有约定或者由于作品使用方式的特性无法指明的除外。

第二十条 著作权法所称已经发表的作品，是指著作权人自行或者许可他人公之于众的作品。

第二十一条 依照著作权法有关规定，使用可以不经著作权人许可的已经发表的作品，不得影响该作品的正常使用，也不得不合理地损害著作权人的合法利益。

第二十二条 依照著作权法第二十三条、第三十三条第二款、第四十条第三款的规定使用作品的付酬标准，由国务院著作权行政管理部门会同国务院价格主管部门制定、公布。

第二十三条 使用他人作品应当同著作权人订立许可使用合同，许可使用的权利是专有使用权的，应当采取书面形式，但是报社、期刊社刊登作品除外。

第二十四条 著作权法第二十四条规定的专有使用权的内容由合同约定，合同没有约定或者约定不明的，视为被许可人有权排除包括著作权人在内的任何人以同样的方式使用作品；除合同另有约定外，被许可人许可第三人行使同一权利，必须取得著作权人的许可。

第二十五条 与著作权人订立专有许可使用合同、转让合同的，可以向著作权行政管理部门备案。

第二十六条 著作权法和本条例所称与著作权有关的权益，是指出版者对其出版的图书和期刊的版式设计享有的权利，表演者对其表演享有的权利，录音录像制作者对其制作的录音录像制品享有的权利，广播电台、电视台对其播放的广播、电视节目享有的权利。

第二十七条 出版者、表演者、录音录像制作者、广播电台、电视台行使权利，不得损害被使用作品和原作品著作权人的权利。

第二十八条 图书出版合同中约定图书出版者享有专有出版权但没有明确其具体内容的，视为图书出版者享有在合同有效期限内和在

合同约定的地域范围内以同种文字的原版、修订版出版图书的专有权利。

第二十九条 著作权人寄给图书出版者的两份订单在 6 个月内未能得到履行，视为著作权法第三十二条所称图书脱销。

第三十条 著作权人依照著作权法第三十三条第二款声明不得转载、摘编其作品的，应当在报纸、期刊刊登该作品时附带声明。

第三十一条 著作权人依照著作权法第四十条第三款声明不得对其作品制作录音制品的，应当在该作品合法录制成为录音制品时声明。

第三十二条 依照著作权法第二十三条、第三十三条第二款、第四十条第三款的规定，使用他人作品的，应当自使用该作品之日起 2 个月内向著作权人支付报酬。

第三十三条 外国人、无国籍人在中国境内的表演，受著作权法保护。

外国人、无国籍人根据中国参加的国际条约对其表演享有的权利，受著作权法保护。

第三十四条 外国人、无国籍人在中国境内制作、发行的录音制品，受著作权法保护。

外国人、无国籍人根据中国参加的国际条约对其制作、发行的录音制品享有的权利，受著作权法保护。

第三十五条 外国的广播电台、电视台根据中国参加的国际条约对其播放的广播、电视节目享有的权利，受著作权法保护。

第三十六条 有著作权法第四十八条所列侵权行为，同时损害社会公共利益，非法经营额 5 万元以上的，著作权行政管理部门可处非法经营额 1 倍以上 5 倍以下的罚款；没有非法经营额或者非法经营额 5 万元以下的，著作权行政管理部门根据情节轻重，可处 25 万元以下的罚款。

第三十七条 有著作权法第四十八条所列侵权行为，同时损害社会公共利益的，由地方人民政府著作权行政管理部门负责查处。

国务院著作权行政管理部门可以查处在全国有重大影响的侵权行为。

第三十八条 本条例自 2002 年 9 月 15 日起施行。1991 年 5 月 24 日国务院批准、1991 年 5 月 30 日国家版权局发布的《中华人民共和国著作权法实施条例》同时废止。

8. 《国务院关于修改〈信息网络传播权保护条例〉的决定》

国务院决定对《信息网络传播权保护条例》作如下修改：

将第十八条、第十九条中的“并可处以 10 万元以下的罚款”修改为：“非法经营额 5 万元以上的，可处非法经营额 1 倍以上 5 倍以下的罚款；没有非法经营额或者非法经营额 5 万元以下的，根据情节轻重，可处 25 万元以下的罚款”。

本决定自 2013 年 3 月 1 日起施行。

《信息网络传播权保护条例》根据本决定作相应修改，重新公布。

信息网络传播权保护条例

第一条 为保护著作权人、表演者、录音录像制作者（以下统称权利人）的信息网络传播权，鼓励有益于社会主义精神文明、物质文明建设的作品的创作和传播，根据《中华人民共和国著作权法》（以下简称著作权法），制定本条例。

第二条 权利人享有的信息网络传播权受著作权法和本条例保护。除法律、行政法规另有规定的外，任何组织或者个人将他人的作品、表演、录音录像制品通过信息网络向公众提供，应当取得权利人许可，并支付报酬。

第三条 依法禁止提供的作品、表演、录音录像制品，不受本条例保护。

权利人行使信息网络传播权，不得违反宪法和法律、行政法规，不得损害公共利益。

第四条 为了保护信息网络传播权，权利人可以采取技术措施。

任何组织或者个人不得故意避开或者破坏技术措施，不得故意制造、进口或者向公众提供主要用于避开或者破坏技术措施的装置或者部件，不得故意为他人避开或者破坏技术措施提供技术服务。但是，法律、行政法规规定可以避开的除外。

第五条 未经权利人许可，任何组织或者个人不得进行下列行为：

（一）故意删除或者改变通过信息网络向公众提供的作品、表演、录音录像制品的权利管理电子信息，但由于技术上的原因无法避免删除或者改变的除外；

（二）通过信息网络向公众提供明知或者应知未经权利人许可被删除或者改变权利管理电子信息的作品、表演、录音录像制品。

第六条 通过信息网络提供他人作品，属于下列情形的，可以不经著作权人许可，不向其支付报酬：

（一）为介绍、评论某一作品或者说明某一问题，在向公众提供的作品中适当引用已经发表的作品；

（二）为报道时事新闻，在向公众提供的作品中不可避免地再现或者引用已经发表的作品；

（三）为学校课堂教学或者科学研究，向少数教学、科研人员提供少量已经发表的作品；

（四）国家机关为执行公务，在合理范围内向公众提供已经发表的作品；

（五）将中国公民、法人或者其他组织已经发表的、以汉语言文字创作的作品翻译成的少数民族语言文字作品，向中国境内少数民族提供；

（六）不以盈利为目的，以盲人能够感知的独特方式向盲人提供已经发表的文字作品；

（七）向公众提供在信息网络上已经发表的关于政治、经济问题的时事性文章；

（八）向公众提供在公众集会上发表的讲话。

第七条 图书馆、档案馆、纪念馆、博物馆、美术馆等可以不经著作权人许可，通过信息网络向本馆馆舍内服务对象提供本馆收藏的合法出版的数字作品和依法为陈列或者保存版本的需要以数字化形式复制的作品，不向其支付报酬，但不得直接或者间接获得经济利益。当事人另有约定的除外。

前款规定的为陈列或者保存版本需要以数字化形式复制的作品，应当是已经损毁或者濒临损毁、丢失或者失窃，或者其存储格式已经过时，并且在市场上无法购买或者只能以明显高于标定的价格购买的作品。

第八条 为通过信息网络实施九年制义务教育或者国家教育规划，可以不经著作权人许可，使用其已经发表作品的片断或者短小的文字作品、音乐作品或者单幅的美术作品、摄影作品制作课件，由制作课件或者依法取得课件的远程教育机构通过信息网络向注册学生提供，但应当向著作权人支付报酬。

第九条 为扶助贫困，通过信息网络向农村地区的公众免费提供中国公民、法人或者其他组织已经发表的种植养殖、防病治病、防灾减灾等与扶助贫困有关的作品和适应基本文化需求的作品，网络服务提供者应当在提供前公告拟提供的作品及其作者、拟支付报酬的标准。

自公告之日起 30 日内，著作权人不同意提供的，网络服务提供者不得提供其作品；自公告之日起满 30 日，著作权人没有异议的，网络服务提供者可以提供其作品，并按照公告的标准向著作权人支付报酬。网络服务提供者提供著作权人的作品后，著作权人不同意提供的，网络服务提供者应当立即删除著作权人的作品，并按照公告的标准向著作权人支付提供作品期间的报酬。

依照前款规定提供作品的，不得直接或者间接获得经济利益。

第十条 依照本条例规定不经著作权人许可、通过信息网络向公众提供其作品的，还应当遵守下列规定：

（一）除本条例第六条第一项至第六项、第七条规定的情形外，不得提供作者事先声明不许提供的作品；

（二）指明作品的名称和作者的姓名（名称）；

（三）依照本条例规定支付报酬；

（四）采取技术措施，防止本条例第七条、第八条、第九条规定的服务对象以外的其他人获得著作权人的作品，并防止本条例第七条规定的服务对象的复制行为对著作权人利益造成实质性损害；

（五）不得侵犯著作权人依法享有的其他权利。

第十一条 通过信息网络提供他人表演、录音录像制品的，应当遵守本条例第六条至第十条的规定。

第十二条 属于下列情形的，可以避开技术措施，但不得向他人提供避开技术措施的技术、装置或者部件，不得侵犯权利人依法享有的其他权利：

（一）为学校课堂教学或者科学研究，通过信息网络向少数教学、科研人员提供已经发表的作品、表演、录音录像制品，而该作品、表演、录音录像制品只能通过信息网络获取；

（二）不以营利为目的，通过信息网络以盲人能够感知的独特方式向盲人提供已经发表的文字作品，而该作品只能通过信息网络获取；

（三）国家机关依照行政、司法程序执行公务；

（四）在信息网络上对计算机及其系统或者网络的安全性能进行测试。

第十三条 著作权行政管理部门为了查处侵犯信息网络传播权的行为，可以要求网络服务提供者提供涉嫌侵权的服务对象的姓名（名称）、联系方式、网络地址等资料。

第十四条 对提供信息存储空间或者提供搜索、链接服务的网络服务提供者，权利人认为其服务所涉及的作品、表演、录音录像制品，侵犯自己的信息网络传播权或者被删除、改变了自己的权利管理电子信息的，可以向该网络服务提供者提交书面通知，要求网络服务提供者删除该作品、表演、录音录像制品，或者断开与该作品、表演、录音录像制品的链接。通知书应当包含下列内容：

（一）权利人的姓名（名称）、联系方式和地址；

（二）要求删除或者断开链接的侵权作品、表演、录音录像制品的名称和网络地址；

（三）构成侵权的初步证明材料。

权利人应当对通知书的真实性负责。

第十五条 网络服务提供者接到权利人的通知书后，应当立即删除涉嫌侵权的作品、表演、录音录像制品，或者断开与涉嫌侵权的作品、表演、录音录像制品的链接，并同时将通知书转送提供作品、表演、录音录像制品的服务对象；服务对象网络地址不明、无法转送的，应当将通知书的内容同时在信息网络上公告。

第十六条 服务对象接到网络服务提供者转送的通知书后，认为

其提供的作品、表演、录音录像制品未侵犯他人权利的，可以向网络服务提供者提交书面说明，要求恢复被删除的作品、表演、录音录像制品，或者恢复与被断开的作品、表演、录音录像制品的链接。书面说明应当包含下列内容：

- （一）服务对象的姓名（名称）、联系方式和地址；
- （二）要求恢复的作品、表演、录音录像制品的名称和网络地址；
- （三）不构成侵权的初步证明材料。

服务对象应当对书面说明的真实性负责。

第十七条 网络服务提供者接到服务对象的书面说明后，应当立即恢复被删除的作品、表演、录音录像制品，或者可以恢复与被断开的作品、表演、录音录像制品的链接，同时将服务对象的书面说明转送权利人。权利人不得再通知网络服务提供者删除该作品、表演、录音录像制品，或者断开与该作品、表演、录音录像制品的链接。

第十八条 违反本条例规定，有下列侵权行为之一的，根据情况承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任；同时损害公共利益的，可以由著作权行政管理部门责令停止侵权行为，没收违法所得，非法经营额 5 万元以上的，可处非法经营额 1 倍以上 5 倍以下的罚款；没有非法经营额或者非法经营额 5 万元以下的，根据情节轻重，可处 25 万元以下的罚款；情节严重的，著作权行政管理部门可以没收主要用于提供网络服务的计算机等设备；构成犯罪的，依法追究刑事责任：

- （一）通过信息网络擅自向公众提供他人的作品、表演、录音录像制品的；
- （二）故意避开或者破坏技术措施的；
- （三）故意删除或者改变通过信息网络向公众提供的作品、表演、

录音录像制品的权利管理电子信息，或者通过信息网络向公众提供明知或者应知未经权利人许可而被删除或者改变权利管理电子信息的作品、表演、录音录像制品的；

（四）为扶助贫困通过信息网络向农村地区提供作品、表演、录音录像制品超过规定范围，或者未按照公告的标准支付报酬，或者在权利人不同意提供其作品、表演、录音录像制品后未立即删除的；

（五）通过信息网络提供他人的作品、表演、录音录像制品，未指明作品、表演、录音录像制品的名称或者作者、表演者、录音录像制作者的姓名（名称），或者未支付报酬，或者未依照本条例规定采取技术措施防止服务对象以外的其他人获得他人的作品、表演、录音录像制品，或者未防止服务对象的复制行为对权利人利益造成实质性损害的。

第十九条 违反本条例规定，有下列行为之一的，由著作权行政管理部门予以警告，没收违法所得，没收主要用于避开、破坏技术措施的装置或者部件；情节严重的，可以没收主要用于提供网络服务的计算机等设备；非法经营额 5 万元以上的，可处非法经营额 1 倍以上 5 倍以下的罚款；没有非法经营额或者非法经营额 5 万元以下的，根据情节轻重，可处 25 万元以下的罚款；构成犯罪的，依法追究刑事责任：

（一）故意制造、进口或者向他人提供主要用于避开、破坏技术措施的装置或者部件，或者故意为他人避开或者破坏技术措施提供技术服务的；

（二）通过信息网络提供他人的作品、表演、录音录像制品，获得经济利益的；

（三）为扶助贫困通过信息网络向农村地区提供作品、表演、录音录像制品，未在提供前公告作品、表演、录音录像制品的名称和作者、表演者、录音录像制作者的姓名（名称）以及报酬标准的。

第二十条 网络服务提供者根据服务对象的指令提供网络自动接入服务，或者对服务对象提供的作品、表演、录音录像制品提供自动传输服务，并具备下列条件的，不承担赔偿责任：

（一）未选择并且未改变所传输的作品、表演、录音录像制品；

（二）向指定的服务对象提供该作品、表演、录音录像制品，并防止指定的服务对象以外的其他人获得。

第二十一条 网络服务提供者为提高网络传输效率，自动存储从其他网络服务提供者获得的作品、表演、录音录像制品，根据技术安排自动向服务对象提供，并具备下列条件的，不承担赔偿责任：

（一）未改变自动存储的作品、表演、录音录像制品；

（二）不影响提供作品、表演、录音录像制品的原网络服务提供者掌握服务对象获取该作品、表演、录音录像制品的情况；

（三）在原网络服务提供者修改、删除或者屏蔽该作品、表演、录音录像制品时，根据技术安排自动予以修改、删除或者屏蔽。

第二十二条 网络服务提供者服务对象提供信息存储空间，供服务对象通过信息网络向公众提供作品、表演、录音录像制品，并具备下列条件的，不承担赔偿责任：

（一）明确标示该信息存储空间是为服务对象所提供，并公开网络服务提供者的名称、联系人、网络地址；

（二）未改变服务对象所提供的作品、表演、录音录像制品；

（三）不知道也没有合理的理由应当知道服务对象提供的作品、表演、录音录像制品侵权；

（四）未从服务对象提供作品、表演、录音录像制品中直接获得经济利益；

（五）在接到权利人的通知书后，根据本条例规定删除权利人认为侵权的作品、表演、录音录像制品。

第二十三条 网络服务提供者服务对象提供搜索或者链接服务，在接到权利人的通知书后，根据本条例规定断开与侵权的作品、表演、录音录像制品的链接的，不承担赔偿责任；但是，明知或者应知所链接的作品、表演、录音录像制品侵权的，应当承担共同侵权责任。

第二十四条 因权利人的通知导致网络服务提供者错误删除作品、表演、录音录像制品，或者错误断开与作品、表演、录音录像制品的链接，给服务对象造成损失的，权利人应当承担赔偿责任。

第二十五条 网络服务提供者无正当理由拒绝提供或者拖延提供涉嫌侵权的服务对象的姓名（名称）、联系方式、网络地址等资料的，由著作权行政管理部门予以警告；情节严重的，没收主要用于提供网络服务的计算机等设备。

第二十六条 本条例下列用语的含义：

信息网络传播权，是指以有线或者无线方式向公众提供作品、表演或者录音录像制品，使公众可以在其个人选定的时间和地点获得作品、表演或者录音录像制品的权利。

技术措施，是指用于防止、限制未经权利人许可浏览、欣赏作品、表演、录音录像制品的或者通过信息网络向公众提供作品、表演、录音录像制品的有效技术、装置或者部件。

权利管理电子信息，是指说明作品及其作者、表演及其表演者、录音录像制品及其制作者的信息，作品、表演、录音录像制品权利人的信息和使用条件的信息，以及表示上述信息的数字或者代码。

第二十七条 本条例自 2006 年 7 月 1 日起施行。

9. 《关于印发〈2013 年打击网络侵权盗版专项治理“剑网行动”实施方案〉的通知》

为加强网络环境下的版权行政执法和监管工作,打击网络侵权盗版行为,净化网络版权环境,促进互联网产业的健康发展,根据国务院 2013 年打击侵犯知识产权和制售假冒伪劣商品工作的部署,国家版权局、国家互联网信息办公室、工业和信息化部、公安部(以下简称“四部门”)制定《2013 年打击网络侵权盗版专项治理“剑网行动”实施方案》,具体内容如下:

一、工作目标

从 2013 年 6 月 20 日开始,利用 4 个月的时间,围绕网络文学、音乐、影视、游戏、动漫、软件等重点领域以及图书、音像制品、电子出版物、网络出版物等重点产品,加强对重点音视频网站、网络销售平台的监管力度,严厉打击各种网络侵权盗版行为。通过查处一批案件、关闭一批违法网站、处理一批违法人员,有力维护网络环境下健康、规范的版权秩序,建立完善互联网版权保护长效工作机制,进一步促进互联网产业繁荣发展。

二、主要任务

(一) 查办一批大案要案。各地版权执法部门、公安机关要确定一批网络侵权盗版重点案件,集中力量、快速查办。对查处的案件确定违法的,要在法定职权范围内加大行政处罚力度;涉嫌犯罪的,要根据“两法衔接”机制及时移送司法机关,强化刑事打击工作力度。

(二) 深入开展对音视频网站的主动监管工作。今年国家版权局将主动监管工作扩大至重点音乐网站,各地版权管理部门要将本地有影响力的较大视频网站和音乐网站纳入到主动监管的范围,明确要求网站按时开展自查自纠活动,加强对监管网站报送材料的监督和审核,指派专门执法人员对网站上传的内容等进行不定期检查,对发现的违

法行为要严肃查处。

（三）加强对移动互联网的版权监管工作。各地版权执法部门要加大对手机等移动设备侵权盗版的查处力度，主动监控通过移动网络传播文学、音乐、影视、游戏、动漫、软件等情况，重点强化对音视频播放软件、游戏软件等领域侵权盗版的打击力度。

（四）加强对网络交易平台的版权监管工作。各地版权管理部门要加强对本地有影响力的各类电子商务交易平台的版权监管工作，要求相关企业建立健全版权保护制度和交易规则，切实采取有效措施积极配合版权执法部门的工作。要积极推动权利人及组织与网络交易平台企业建立版权保护协作机制。版权执法部门要严厉查处各种利用网络交易平台销售侵权盗版制品等违法行为，涉嫌犯罪的，要及时移送司法机关追究刑事责任。

（五）健全完善督办协调机制。国家版权局将会同国家互联网信息办公室、工业和信息化部、公安部联合挂牌督办一批网络侵权盗版重点案件，对列入督办范围的案件采取派员参加专案组、巡视督促、跨区域协调等方式，积极构建迅速、顺畅、便捷、高效的办案工作机制。

（六）加强法制宣传教育工作。要通过曝光一批网络侵权盗版典型案件，深入开展警示教育工作，对检查、督察中发现的违法企业、个人进行法制教育，帮助企业树立保护版权、“先授权、后传播”的法律意识，使其自觉遵守相关法律法规。

三、重点工作

（一）提高查处案件的数量和质量。各地要发布举报奖励公告，充分发挥权利人组织的积极性，鼓励社会各界积极提供案件线索。要继续加大对网络侵权盗版案件的处罚力度，在进一步提高办案的数量和质量上下工夫。尤其是要重点打击一批人民群众反响强烈、社会影响力大的侵权盗版网站，确保在办理大案要案方面取得实质性突破。

（二）进一步加大刑事打击力度。各地要深入落实“两法衔接”机制的要求，版权执法部门在执法检查 and 接受举报投诉时，发现网站侵权盗版行为涉嫌犯罪的，要及时向公安机关移送，并积极配合公安机关深入打击网络侵权盗版犯罪行为。

（三）突出重点工作领域。要重点围绕网络文学、音乐、影视、游戏、动漫、软件以及网络销售平台等领域，严厉打击未经许可非法上载、传播他人作品以及通过电子商务平台销售盗版制品等违法行为；严厉打击故意为侵权盗版分子提供搜索链接、信息存储空间以及服务器托管、网络接入等服务的违法行为；严厉打击利用手机等移动设备、电视机顶盒、电视棒和音视频播放器等软硬件工具侵权盗版的违法犯罪活动。

四、职责分工

（一）健全领导及工作机构。为加强对本次专项行动的组织与领导，四部门成立“全国打击网络侵权盗版专项治理工作领导小组”，新闻出版广电总局副局长、国家版权局副局长阎晓宏担任组长，领导小组成员由国家版权局版权管理司、国家互联网信息办公室网络新闻协调局、工业和信息化部电信管理局、公安部治安管理局相关司局级干部组成，统一部署重大任务，协调解决相关问题，指导各地开展相关工作。领导小组办公室设在国家版权局版权管理司。各地要成立相应的工作领导小组，协调指导本地区工作的开展，组成情况请于7月10日前同工作计划一并上报领导小组办公室。

（二）版权管理部门负责专项治理行动的牵头工作。版权管理部门要协调互联网信息内容主管部门、通信管理部门、公安机关开展工作；负责组织梳理网上侵权信息，收集案件线索，查处违法行为，移送涉嫌犯罪案件，提请通信管理部门予以暂停网站接入或者关闭网站。开展音视频网站主动监管及网络交易平台版权监管工作；组织专项治理行动的宣传和奖励工作；协调、指导文化市场综合执法机构开展版权执法工作。

（三）互联网信息内容主管部门负责指导、协调、督促有关部门加强网络内容管理、依法从严查处侵权盗版违法网站，利用版权手段加强对网络内容的监管。

（四）通信管理部门配合版权、公安部门开展打击网络侵权盗版工作，协助开展网络侵权盗版案件调查取证工作，协助提供查处网络侵权盗版案件涉及网站的备案信息，对经版权、公安部门查处且侵权盗版情节严重的网站依法吊销电信业务经营许可证或者注销备案，并通知相关接入服务商停止为其提供网站接入服务。组织开展行业自律活动。

（五）公安机关要加大对网络环境下侵权盗版涉嫌犯罪案件的线索收集、立案查处工作，及时受理版权部门移送的涉嫌犯罪的案件，进一步加大对侵权盗版犯罪案件的刑事打击力度。

五、工作要求

（一）高度重视，列入考核。各地要高度重视今年的“剑网行动”，国家版权局等四部门已将该项工作列入2013年“双打”工作考核的重点，将适时向国务院打击侵权假冒工作领导小组报告考核情况并反馈各地党委政府。

（二）做好计划，周密部署。各地版权管理部门要根据本地情况，协调版权执法、互联网信息内容主管、通信管理、公安部门，周密部署、制定具体的详尽的工作计划，于7月10日前上报国家版权局版权管理司。

（三）创新工作方法，加强制度建设。各地要在执法技术手段和管理方式等方面进行创新，通过约谈网站负责人、督办重点案件等方式，督促问题网站进行认真整改。要不断总结工作经验，健全完善网络版权执法和监管工作的各项制度，逐步建立统一、规范的版权执法监管工作流程。

（四）构建多部门共同参与的联动工作机制。各地版权、互联网信息内容主管、通信、公安部门要进一步加强配合，联合办案，按照分工认真开展工作。各地版权管理部门要做好工作部署和协调，版权执法部门要切实承担版权行政执法任务，互联网信息内容主管部门要利用版权手段加强网络监管并做好指导、协调和督促工作，通信管理部门要配合加大对违法网站的查处力度，公安部门要加大网络侵权盗版案件的侦查力度。

（五）加强信息报送工作。各地要高度重视执法信息汇总和上报工作。省级版权局、文化市场执法总队整理、汇总地方各级版权行政执法部门案件查处及音视频网站主动监管情况，统一填写附件 1、附件 2、附件 3、附件 4，从 7 月起每月 15 日前、30 日前向国家版权局版权管理司各报送 1 次；省级互联网信息内容主管部门、通信管理局、公安（厅）局分别整理、汇总地方各级互联网信息内容主管、通信管理、公安部门查处或配合查处案件情况，统一填写附件 3，按月分别报送到国家互联网信息办公室网络新闻协调局、工信部电信管理局、公安部治安管理局。各地、各部门上报的执法情况材料将作为评价各地、各部门执法工作以及奖励查处侵权盗版有功单位和个人的重要依据。

六、实施步骤

2013 年打击网络侵权盗版专项治理“剑网行动”分四个阶段进行。

（一）工作部署阶段（6 月 20 日—7 月 10 日）。1. 四部门召开新闻发布会，全面启动今年“剑网行动”。2. 各地积极落实文件要求，上报专项治理行动工作领导小组办公室组成情况和具体工作安排，各地确定主动监管网站名单。3. 制定专项行动宣传方案，组织媒体宣传相关法律法规与政策，宣传打击网络侵权盗版典型案例。

（二）自查自纠与收集案源阶段（7 月 11 日—7 月 31 日）。1. 进行自查自纠，组织引导合法经营的互联网企业和重点网站开展自查自

纠活动，查找侵权盗版隐患。2. 收集案件线索，组织动员国内外权利人组织和社会公众投诉举报网络侵权盗版行为，充分利用国家版权局的举报电话等途径以及各地的投诉举报平台，收集案件线索。3. 开展执法培训，组织各有关部门行政执法人员的培训工作。编辑印发专项治理行动法律政策、业务指南和案例汇编。

（三）集中治理阶段（8月1日—9月30日）。1. 限期整改，各地有关部门要责令本地确定为主动监管的互联网企业和网站对自查出来的问题进行限期整改，对未按期完成整改的要依法查处。2. 集中执法，四部门确定一批重点案件进行挂牌督办。各级版权、互联网信息内容主管、通信管理、公安部门要根据上级移交和自行收集到的案件线索开展打击行动，要充分发挥联合执法机制，依法加大行政处罚力度，加强涉嫌犯罪案件的移送工作，集中办理一批大案要案，始终保持集中打击的高压态势。

（四）督察总结阶段（10月1日—10月20日）。1. 各地汇总专项治理工作情况，形成总结报告，于10月31日前上报国家版权局版权管理司。2. 开展督察，四部门对重点地区、重点企业进行督导检查，调研专项治理行动开展的情况。3. 新闻通报，四部门联合召开新闻通气会，对外宣传我国政府为打击网络侵权盗版所做的努力和取得的成绩；通报专项治理行动中的典型经验和典型案例。4. 总结奖励，四部门及时总结专项治理行动成果，依据《举报、查处侵权盗版行为奖励暂行办法》对专项治理行动中工作突出的单位和个人予以奖励，纳入2013年度版权执法有功单位和个人奖励范围，对重大典型案件进行专项奖励。

10. 《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》

第一条 具有下列情形之一的，应当认定为刑法第二百四十六条

第一款规定的“捏造事实诽谤他人”：

（一）捏造损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

（二）将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

明知是捏造的损害他人名誉的事实，在信息网络上散布，情节恶劣的，以“捏造事实诽谤他人”论。

第二条 利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第一款规定的“情节严重”：

（一）同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的；

（二）造成被害人或者其近亲属精神失常、自残、自杀等严重后果的；

（三）二年内曾因诽谤受过行政处罚，又诽谤他人的；

（四）其他情节严重的情形。

第三条 利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第二款规定的“严重危害社会秩序和国家利益”：

（一）引发群体性事件的；

（二）引发公共秩序混乱的；

（三）引发民族、宗教冲突的；

（四）诽谤多人，造成恶劣社会影响的；

（五）损害国家形象，严重危害国家利益的；

（六）造成恶劣国际影响的；

（七）其他严重危害社会秩序和国家利益的情形。

第四条 一年内多次实施利用信息网络诽谤他人行为未经处理，诽谤信息实际被点击、浏览、转发次数累计计算构成犯罪的，应当依法定罪处罚。

第五条 利用信息网络辱骂、恐吓他人，情节恶劣，破坏社会秩序的，依照刑法第二百九十三条第一款第（二）项的规定，以寻衅滋事罪定罪处罚。

编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第（四）项的规定，以寻衅滋事罪定罪处罚。

第六条 以在信息网络上发布、删除等方式处理网络信息为由，威胁、要挟他人，索取公私财物，数额较大，或者多次实施上述行为的，依照刑法第二百七十四条的规定，以敲诈勒索罪定罪处罚。

第七条 违反国家规定，以营利为目的，通过信息网络有偿提供删除信息服务，或者明知是虚假信息，通过信息网络有偿提供发布信息等服务，扰乱市场秩序，具有下列情形之一的，属于非法经营行为“情节严重”，依照刑法第二百二十五条第（四）项的规定，以非法经营罪定罪处罚：

（一）个人非法经营数额在五万元以上，或者违法所得数额在二万元以上的；

（二）单位非法经营数额在十五万元以上，或者违法所得数额在五万元以上的。

实施前款规定的行为，数额达到前款规定的数额五倍以上的，应

当认定为刑法第二百二十五条规定的“情节特别严重”。

第八条 明知他人利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等犯罪，为其提供资金、场所、技术支持等帮助的，以共同犯罪论处。

第九条 利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营犯罪，同时又构成刑法第二百二十一条规定的损害商业信誉、商品声誉罪，第二百七十八条规定的煽动暴力抗拒法律实施罪，第二百九十一条之一规定的编造、故意传播虚假恐怖信息罪等犯罪的，依照处罚较重的规定定罪处罚。

第十条 本解释所称信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及向公众开放的局域网络。

11. 《关于加强移动智能终端管理的通知》

一、本通知所称移动智能终端是指接入公众移动通信网络、具有操作系统、可由用户自行安装应用程序的移动通信终端产品。

二、申请进网许可的移动智能终端应当符合通信行业标准有关移动智能终端安全的基本要求，检测机构在进网检测时应当依据相关标准进行检测。

三、生产企业申请移动智能终端进网许可时，应当在申请材料中提供操作系统版本、预置应用软件基本配置信息。

四、生产企业不得在移动智能终端中预置具有以下性质的应用程序：

（一）未向用户明示并经用户同意，擅自收集、修改用户个人信息的；

（二）未向用户明示并经用户同意，擅自调用终端通信功能，造成流量消耗、费用损失、信息泄露等不良后果的；

（三）影响移动智能终端正常功能或通信网络安全运行的；

（四）含有《中华人民共和国电信条例》禁止发布、传播的信息内容的；

（五）其他侵害用户个人信息安全和合法权益以及危害网络与信息安全的。

五、获得进网许可的移动智能终端新增预置应用软件，或者操作系统升级发生的变化涉及进网检测中终端基本安全要求项目的，生产企业应当向工业和信息化部报备。

六、生产企业应当在其获得进网许可的产品或其包装显著位置标注工业和信息化部规定的进网许可标志查验网址。

七、本通知自 2013 年 11 月 1 日起执行。

附录B 地方层面立法摘编

1. 《北京市信息化促进条例》

（涉及互联网立法方面）

第四章 信息技术推广应用

第二十四条 市和区、县人民政府应当采取措施推动企业和个人利用信息网络从事商务活动，引导社会逐步建立、完善信用体系和网上支付、物流配送系统，鼓励电子商务服务提供商的发展。

市人民政府有关部门应当制定以中小企业为主的企业信息化发展指南，建设面向中小企业的公共信息服务平台。

第二十五条 本市统筹城乡信息化发展，加大公共财政投入，支持农村信息基础设施和农村综合信息平台建设和运行维护，推进农村现代远程教育；鼓励通过信息化手段为农民提供生产、生活实用信息服务，开发、利用涉农信息资源，开展面向农民的信息化知识和技能培训。

电信、广播、电视等公共服务单位应当采取措施加强农村信息网络服务。

第二十六条 在本市从事互联网信息服务活动的，应当按照国家规定办理相应许可或者履行备案手续。

利用互联网从事经营活动的单位和个人应当依法取得营业执照，并在网站主页面上公开经营主体信息、已取得相应许可或者备案的证

明、服务规则和服务流程等相应信息。

第二十七条 电子商务服务提供商应当对利用其网站从事经营活动的经营主体的身份信息、合法经营凭证和反映交易信用状况的材料进行核查，并对相关信息做好数据备份，便于当事人和有关部门查询、核对。

电子商务服务提供商应当建立投诉受理机制，对利用其网站从事的经营活动进行监督，配合政府有关部门的管理活动，但不得妨碍相关经营主体开展正常交易活动。

第二十八条 本市各级国家机关应当定期组织本单位工作人员学习电子政务相关知识，开展电子政务技能培训。

第二十九条 本市建设统一的电子政务网络，促进相关业务应用系统的互联互通。

本市各级国家机关的业务应用系统，凡不宜通过互联网实现的，必须依托全市统一的电子政务网络；需要接入全市统一的电子政务网络的，应当符合有关规范，并经市或者区、县信息化主管部门审查同意。

各级国家机关不得新建专用网络，已经建成的专用网络应当按照规划和标准逐步调整，接入电子政务网络。

第三十条 本市国家机关的网站应当按照规定与本市政务门户网站建立链接，统一网站风格、标识和建设运行维护技术标准。

本市国家机关在互联网上注册域名的，应当遵守国家和本市的相关规定，并经过市信息化主管部门的审核。

第三十一条 市和区、县信息化主管部门组织开展信息化成果展示和交流，对先进的信息技术、产品进行示范推广。

第五章 信息安全保障

第三十二条 本市对网络与信息系统按照国家和本市有关规定实行安全等级保护制度。

网络与信息系统的建设单位和运行维护单位应当按照国家信息安全等级保护管理规范和技术标准确定本单位网络与信息系统的安全保护等级，并按照国家和本市有关规定进行备案、审批。

第三十三条 信息系统的建设单位和运行维护单位应当根据确定的安全保护等级，按照国家信息安全等级保护管理规范和技术标准，保证相应投入，同步开展信息系统安全建设或者改建工作；建设完成后，建设单位和运行单位应当按照国家有关规定开展安全等级技术测评工作，并根据结果采取措施保障网络与信息系统的的功能。

第三十四条 本市网络与信息系统的建设单位和运行维护单位应当加强安全管理，并制定网络与信息系统安全事件应急预案，定期进行演练。

发生网络与信息系统安全事故后，相关单位应当迅速采取措施降低损害程度，防止事故扩大，保存相关记录，并按照规定及时向同级信息化主管部门报告。

市和区、县人民政府有关部门应当组织制定相关行业的网络与信息系统安全事件应急预案，组织、协调有关单位做好应急预案的落实工作。

第三十五条 本市组建公共服务网络与信息系统信息安全应急救援服务体系，建立信息安全情况通报和协调机制，为发生公共服务信息安全事件的单位提供救援服务，为全市应急指挥体系提供网络与信息系统安全保障。

第三十六条 任何单位和个人不得利用网络与信息系统从事危害

国家安全，扰乱公共秩序，损害公民、法人和其他组织的合法权益，危害网络和信息系统安全以及散布、传播违法信息等活动。

第三十七条 涉及国家秘密的信息化工程的管理，按照国家保密有关规定执行。

第七章 法律责任

第四十三条 违反本条例第十一条规定，未经资质认证的单位承揽、以其他单位名义承揽相应领域的信息化工程，或者已经资质认证的单位超越本单位资质等级承揽信息化工程的；由市或者区、县信息化主管部门给予警告，责令限期改正；情节严重的，处以1万元以上10万元以下罚款。

第四十四条 违反本条例第三十四条规定，未按要求制定网络与信息系统安全事件应急预案，或者对网络与信息系统安全事故情况隐瞒不报、谎报或者拖延不报的，由市或者区、县信息化主管部门责令限期改正，并可处3万元以下罚款。

第四十五条 违反本条例规定，有下列行为之一的，由有关部门依照《中华人民共和国政府信息公开条例》、《中华人民共和国计算机信息系统安全保护条例》等有关规定责令改正，给予警告或者责令停机整顿，并对直接负责的主管人员和其他直接责任人员依法处理：

（一）违反第十九条规定，未按照国家和本市的规定公开政务信息的；

（二）违反第三十二条规定，网络与信息系统的建设单位和运行维护单位未依法进行安全保护等级备案、审批的；

（三）违反第三十三条规定，未进行网络与信息系统安全建设或者改建工作，或者未进行网络与信息系统安全等级技术测评的。

第四十六条 违反本条例规定，有下列行为之一的，市或者区、

县信息化主管部门可以对责任单位给予通报批评；造成重大损失的，依照有关法律、法规予以处理：

（一）违反第十七条规定，没有正当理由，重复采集政务信息资源目录内信息的；

（二）违反第二十九条第二款规定，未经审查同意擅自接入电子政务网络的。

第四十七条 对于信息化发展过程中有危害国家安全，扰乱公共秩序，损害公民、法人和其他组织的合法权益，危害网络与信息系统安全以及散布、传播违法信息等活动的，由国家安全、公安、保密、工商以及其他部门依法处理；构成犯罪的，依法追究刑事责任。

第四十八条 市和区、县信息化主管部门以及其他有关部门的工作人员在信息化工作中徇私舞弊、滥用职权、玩忽职守的，由有关部门依法给予行政处分；构成犯罪的，依法追究刑事责任。

2. 《北京市微博客发展管理若干规定》

第一条 为了规范微博客服务的发展管理，维护网络传播秩序，保障信息安全，保护互联网信息服务单位和微博客用户的合法权益，满足公众对互联网信息的需求，促进互联网健康有序发展，根据《中华人民共和国电信条例》、《互联网信息服务管理办法》等法律、法规、规章，结合本市实际情况，制定本规定。

第二条 本市行政区域内的网站开展微博客服务及其微博客用户，应当遵守本规定。

第三条 本市微博客发展管理坚持积极利用、科学发展、依法管理、确保安全的原则，促进微博客的建设、运用，发挥微博客服务社会的积极作用。

第四条 网站开展微博客服务，应当遵守宪法、法律、法规、规章，坚持诚信办网、文明办网，积极传播社会主义核心价值观体系，传播社会主义先进文化，为构建社会主义和谐社会服务。

第五条 本市制定微博客服务发展规划，规定开展微博客服务网站的总量、结构和布局。

第六条 本市行政区域内网站开展微博客服务，应当在申请电信业务经营许可或者履行非经营性互联网信息服务备案手续前，依法向市互联网信息内容主管部门提出申请，并经审核同意。

第七条 开展微博客服务的网站，应当遵守有关法律、法规、规章和下列规定：

- （一）建立健全微博客信息安全管理制；
- （二）根据微博客用户数量和信息量，确定负责信息安全的机构，配备具有相应专业知识和技能的人员；
- （三）落实技术安全防控措施；
- （四）建立健全用户信息安全管理制，保障用户信息安全，严禁泄露用户信息；
- （五）建立健全虚假信息揭露制，及时公布真实信息；
- （六）不得向未经电信业务经营许可或者未履行非经营性互联网信息服务备案的网站提供信息接口；
- （七）不得制造虚假的微博客用户；
- （八）对传播有害信息的用户予以制止、限制，发现构成违反治安管理行为，或者发现涉嫌犯罪的，及时向公安机关报告；
- （九）协助、配合有关部门开展管理工作。

第八条 开展微博客服务的网站，应当建立健全信息内容审核制

度，对微博客信息内容的制作、复制、发布、传播进行监管。

第九条 任何组织或者个人注册微博客账号，制作、复制、发布、传播信息内容的，应当使用真实身份信息，不得以虚假、冒用的居民身份信息、企业注册信息、组织机构代码信息进行注册。

网站开展微博客服务，应当保证前款规定的注册用户信息真实。

第十条 任何组织或者个人不得违法利用微博客制作、复制、发布、传播含有下列内容的信息：

- （一）违反宪法确定的基本原则的；
- （二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- （三）损害国家荣誉和利益的；
- （四）煽动民族仇恨、民族歧视，破坏民族团结的；
- （五）破坏国家宗教政策，宣扬邪教和封建迷信的；
- （六）散布谣言，扰乱社会秩序，破坏社会稳定的；
- （七）散布淫秽、色情、赌博、暴力、恐怖或者教唆犯罪的；
- （八）侮辱或者诽谤他人，侵害他人合法权益的；
- （九）煽动非法集会、结社、游行、示威、聚众扰乱社会秩序的；
- （十）以非法民间组织名义活动的；
- （十一）含有法律、行政法规禁止的其他内容的。

第十一条 市人民政府新闻管理部门、市公安局、市通信管理部门、市互联网信息内容主管部门按照各自职责，做好微博客发展管理的相关工作。

第十二条 网络媒体协会、网络行业协会、通信行业协会等行业

组织应当建立健全微博客行业自律制度，指导网站建立健全微博客服务规范，并对网站从业人员进行培训教育。

第十三条 对违反本规定的行为，任何组织和个人都可以向市人民政府新闻管理部门、市公安机关、市通信管理部门、市互联网信息内容主管部门举报，接到举报的部门应当及时依法处理。

第十四条 对违反本规定的网站和微博客用户，由市人民政府新闻管理部门、市公安机关、市通信管理部门、市互联网信息内容主管部门按照有关法律、法规、规章进行处理。

第十五条 本规定公布前已开展微博客服务的网站，应当自本规定公布之日起三个月内依照本规定向市互联网信息内容主管部门申办有关手续，并对现有用户进行规范。

第十六条 本规定自公布之日起施行。

3. 《北京市公共服务网络与信息系统安全管理规定》

第一条 为加强本市公共服务网络与信息系统（以下简称网络与信息系统）的安全管理，根据国家有关规定，结合本市实际情况，制定本规定。

第二条 本市网络与信息系统的建设和运行维护单位（以下简称运营单位）应当做好网络与信息系统安全工作，保障网络与信息系统安全可靠运营。

本规定所称公共服务网络与信息系统，是指由本市行政机关和企事业单位为社会提供的政务、交通、医疗卫生、供水、供电、供气、供热、通信、广播电视以及其他公共服务的网络与信息系统。

第三条 市和区、县信息化主管部门对本行政区域内的网络与信息系统安全工作负责综合协调和监督管理。

公安、国家安全和质量技术监督等政府有关部门，按照各自职责分工，依法对网络与信息系统安全相关工作实施监督管理。

第四条 运营单位应当加强对本单位网络与信息系统的安全管理，做好下列工作：（一）明确网络与信息系统安全工作的主要负责人和主管机构，并配备具有相应能力的工作人员；（二）建立健全网络与信息系统安全管理责任制，制定管理制度和操作规程，并定期检查落实情况；（三）保障网络与信息系统安全的资金投入；（四）定期进行网络与信息系统安全教育和培训。

第五条 市信息化主管部门应当会同政府有关部门统一规划和组织建设本市网络与信息系统的的功能测评、电子认证、灾难备份和应急处理等安全基础设施。

第六条 本市对网络与信息系统实行安全等级保护。

网络与信息系统安全等级分为五级：

（一）第一级为自主保护级，由运营单位进行自主保护；

（二）第二级为指导保护级，由运营单位在有关主管部门的指导下进行保护；

（三）第三级为监督保护级，由运营单位在备案监督部门的监督下进行保护；

（四）第四级为强制保护级，由运营单位在备案监督部门的强制下进行保护；

（五）第五级为专控保护级，由运营单位在备案监督部门的专控下进行保护。

第七条 运营单位应当按照安全等级保护制度的管理规范和技术标准确定本单位网络与信息系统的的功能等级，并根据安全等级保护制度的要求进行建设。

网络与信息系统安全等级确定为第三级、第四级、第五级的，运营单位应当将安全等级确定情况报送备案。其中，涉及电子政务的网络与信息系统运营单位，应当报市信息化主管部门备案；其他的运营单位应当报市公安部门备案。

市信息化主管部门、市公安部门应当在 30 日内对备案单位的网络与信息系统安全等级确定情况进行评估，并提出审查意见。

第八条 运营单位选用网络与信息系统相关安全产品或者选择安全测评、电子认证等服务时，应当符合国家和本市有关网络与信息系统安全管理的技术规范。

使用财政资金投资建设的网络与信息系统选用安全产品和服务时，应当依法实行政府采购。

第九条 运营单位应当依据网络与信息系统安全管理要求，对信息系统和信息数据进行备份。

第十条 运营单位应当制定网络与信息系统安全事件应急预案，并定期进行演练。

市和区、县人民政府有关行政主管部门应当组织制定相关行业的网络与信息系统安全事件应急预案，组织、协调有关单位做好应急预案的落实工作。

第十一条 发生网络与信息系统安全事件后，运营单位应当迅速采取措施降低损害程度，防止事件扩大，保存相关记录，并按规定要求及时向同级信息化主管部门报告。

第十二条 本市组建信息安全应急救援服务体系，为发生信息安全事件的单位提供救援服务。信息安全应急救援服务组织应当公布救援电话，在接到救援请求时，及时提供救援服务。

第十三条 运营单位违反本规定，有下列情形之一的，由市或者区、

县信息化主管部门责令限期改正，给予警告，视情节轻重处3万元以下罚款：

（一）违反本规定第四条规定，未按要求建立并落实安全管理制度的；

（二）违反本规定第九条规定，未按要求对信息系统和信息数据进行备份的；

（三）违反本规定第十条第一款规定，未按要求制定网络与信息系统安全事件应急预案的；

（四）违反本规定第十一条规定，对网络与信息系统安全事件情况隐瞒不报、谎报或者拖延不报的。

行政机关违反前款规定的，市或者区、县信息化主管部门可以对责任单位给予通报批评；造成重大损失的，由上级主管部门或者监察机关依法追究责任单位主要负责人和有关责任人员的行政责任。

第十四条 对于有危害公共安全、国家安全、泄露国家秘密以及其他违反法律、法规和规章规定行为的，由公安、国家安全、保密以及其他监督管理部门依法处理；构成犯罪的，依法追究刑事责任。

第十五条 国家和本市对涉及国家秘密、国家安全的网络与信息系统有特殊规定的，从其规定。

第十六条 本规定自2006年1月1日起施行。

4. 《上海市促进电子商务发展规定》

第一条 为了促进本市电子商务发展，根据有关法律、行政法规，结合本市实际，制定本规定。

第二条 本市行政区域内促进电子商务发展及其相关管理活动，适用本规定。

第三条 本规定所调整的电子商务，是通过互联网进行销售商品、提供服务等的经营活动。

本规定所称的从事电子商务的企业，包括在互联网上建立电子商务应用服务平台（以下简称电子商务平台）的企业、在电子商务平台内从事经营活动的企业、在互联网上建立网站销售商品或者提供服务的企业以及其他通过互联网从事经营活动的企业。

第四条 本市促进电子商务发展，遵循政府推动、企业主导、市场运作、依法规范的原则。

第五条 市经济信息化行政管理部门负责组织、指导和协调电子商务的推广以及相关的信息化推进、管理工作。

市商务行政管理部门负责拟定商务领域电子商务发展的政策、措施、标准、规则，做好相关推进、管理工作。

其他有关行政管理部门根据各自职责，做好促进电子商务发展和相关管理工作。

区、县人民政府及其相关行政管理部门按照各自职责，做好促进电子商务发展工作。

第六条 市经济信息化行政管理部门会同市发展改革、商务等行政管理部门编制本市电子商务发展规划，纳入本市信息化发展规划，并与相关产业发展规划相衔接。

第七条 市经济信息化行政管理部门会同有关行政管理部门根据本市国民经济和社会发展中长期规划以及社会对基础通信网络的需求，组织编制信息基础设施发展规划。

电信运营企业应当增强通信服务能力，提高通信服务水平。

第八条 本市优先支持下列促进电子商务发展的项目：

（一）先进制造业和现代服务业等重点领域电子商务平台的建设。

（二）电子支付、安全认证、信用服务、物流信息等电子商务服务体系的建设和。

（三）电子商务关键技术的研发和推广应用。

前款所列项目的支持办法，由市人民政府另行制定。

第九条 本市政府采购应当优先采用电子化方式，利用相关电子商务平台，开展信息发布和交易、支付、信用评估等活动。

第十条 市经济信息化、商务、发展改革、财政、税务、教育、科技、统计、人力资源社会保障、金融服务等行政管理部门应当按照各自职责，做好下列促进电子商务发展工作：

（一）制定并及时公布符合本规定第八条所列项目的项目指南。

（二）建立电子商务统计制度，完善电子商务统计指标体系，定期发布电子商务发展报告。

（三）组织开展电子商务基础知识和应用技能的培训；培养和引进适应电子商务发展的各类专业人才。

（四）推动电子商务领域的信用建设，建立市场诚信公共服务平台。

（五）采取创业指导、信息咨询、技术服务等措施，扶持中小企业通过电子商务平台开展经营活动。

（六）推动建立适应电子商务发展的风险投资、融资担保、责任保险等机制，推动电子商务发展。

（七）推动企业运用电子商务开拓国内外市场，促进跨国、跨地区电子商务合作交流。

（八）推进电子签名与认证技术的应用，支持电子认证服务机构实现交叉认证。

（九）鼓励银行推广和完善电子银行服务业务，支持发展第三方电子支付服务机构。

第十一条 本市各级行政管理部门应当推进实施适应电子商务发展的管理方式，建立和完善电子化的管理系统、信息共享系统和公共服务平台。

市工商、质量技监等行政管理部门应当建立和完善企业注册、组织机构代码、各类许可证等信息的电子查询系统，并根据政府信息公开的规定提供相关信息的网上查询服务。

第十二条 本市相关行业协会应当按照法律、法规的规定，发挥行业自律和行业服务作用，做好下列促进电子商务发展的工作：

（一）制定和完善行业内电子商务争议处理的规则和程序，协调会员之间、会员与非会员之间或者会员与消费者之间的争议事项。

（二）建立行业内电子商务信用评价制度，推进相关信用评价的互通、互联、互认。

（三）向政府有关部门提出制定电子商务相关标准的建议，推动会员单位制定电子商务相关标准并组织实施。

（四）引导会员运用电子商务平台组织市场拓展，发布市场信息，推介行业产品或者服务。根据会员需求，开展行业电子商务应用培训和咨询服务。

（五）研究制定适应电子商务特征的合同示范文本，并推广应用。

（六）其他可以促进电子商务发展的工作。

市人民政府有关行政管理部门应当支持相关行业协会开展前款规定的活动，并提供指导。

第十三条 本市建立和完善统一的电子口岸数据交换平台，实现

对外贸易监管数据电子化报送，提高通关效率。

市口岸、经济信息化和商务行政管理部门应当推进电子口岸数据交换平台应用功能的拓展，为对外贸易电子商务提供支持和便利。

第十四条 从事电子商务的企业应当根据国家有关规定取得相关证照，并在其经营网页上公开以下信息：

- （一）营业执照、组织机构代码以及其他与经营资质相关的资料。
- （二）互联网信息服务许可登记或者备案登记的电子验证标识。
- （三）所经营产品依法应当取得的许可、认证证书以及产品名称、生产者等产品信息。
- （四）经营地址、邮政编码、电话号码、电子信箱等联系信息。

第十五条 从事电子商务的企业应当根据国家有关规定，对电子商务活动中的交易标的、数量、质量、价款、履行方式、违约责任等信息进行记录并保存，保存时间不得少于两年，但国家另有规定的除外。

市经济信息化行政管理部门应当推动建立第三方电子数据保存系统，提供交易信息的保存、查询等服务。

鼓励从事电子商务的企业委托第三方电子数据保存系统保存交易信息。

第十六条 企业在从事电子商务的过程中需要采集个人信息的，应当向信息提供者说明采集目的和使用范围，不得收集与该经营事项无关的个人信息，不得超越范围使用所获得的个人信息。

对获得的个人信息应当采取必要的安全措施，保障其不被泄露；未经信息提供者同意，不得将所获得的个人信息向第三方转让。

市质量技监行政管理部门应当会同市经济信息化行政管理部门组织制定电子商务个人信息采集的相关标准。

第十七条 从事电子商务的企业在互联网上以商业广告等公示方式，对商品或者服务的质量、价格、售后责任等向消费者作出许诺的，其提供的商品或者服务的质量、价格、售后责任等应当与许诺相一致。消费者受上述许诺引导而购买商品或者接受服务的，从事电子商务的企业应当将该许诺作为约定的内容。

第十八条 在互联网上建立电子商务平台的企业应当按照国家规定，建立健全网络与信息安全保障制度，保障电子商务平台安全。

在互联网上建立电子商务平台的企业，对经营过程中知悉的在其电子商务平台内从事经营活动企业的经营信息，应当按照约定，承担保密义务。

在互联网上建立电子商务平台的企业应当建立经营证照核查制度，对在其电子商务平台内从事经营活动的企业的相关经营证照进行查看、核对，并留存复制件。

在互联网上建立电子商务平台的企业发现在其电子商务平台内从事各类违法行为的，应当予以制止，并立即向有关部门报告。

第十九条 市工商、经济信息化、商务等行政管理部门应当会同市消费者权益保护委员会，建立并完善下列与电子商务相关的消费者权益保护机制：

（一）消费投诉处理机制。完善消费投诉系统，与在互联网上建立电子商务平台的企业建立消费投诉联网，为消费者投诉提供便利和指导。

（二）信用评价机制。支持在互联网上建立电子商务平台的企业对在其电子商务平台内从事经营活动的企业进行信用评价，向消费者提供信用评价信息。

（三）消费信息公布机制。发布电子商务相关消费警示信息和消

费指导信息，并披露经核实的消费者投诉情况。

从事电子商务的企业向消费者出具购货凭证或者服务单据，应当符合国家有关规定或者商业惯例；征得消费者同意的，可以以电子化形式出具。电子化的购货凭证或者服务单据，可以作为消费者权益保护组织处理消费纠纷投诉的依据。鼓励在互联网上建立电子商务平台的企业为平台内从事经营活动的企业提供电子化购货凭证或者服务单据的统一格式文本。

第二十条 违反本规定的行为，法律、法规有处罚规定的，依照法律、法规的规定处罚。

从事电子商务的企业违反本规定有下列情形之一的，由工商行政管理部门责令限期改正，可以处以警告；逾期不改正的，处以一千元以上一万元以下的罚款：

- （一）未按规定在其经营网页上公开营业执照信息的。
- （二）未按规定提供购货凭证或者服务单据的。

第二十一条 行政管理部门的直接主管人员或者其他责任人员，玩忽职守、滥用职权、徇私舞弊的，由其所在单位或者上级行政主管部门依法给予行政处分。构成犯罪的，依法追究刑事责任。

第二十二条 本规定自2009年3月1日起施行。

5. 广东省《关于进一步加强防范互联网上有害信息传播的通知》

各互联网业务经营者、互联网信息服务提供者：

为进一步加强和落实互联网信息安全管理，健全互联网信息安全管理制度，维护社会稳定，预防和坚决制止网上有害信息的传播，现就有关问题通知如下：

一、互联网业务经营者要遵纪守法，牢固树立大局意识和稳定意识，严格按照“谁经营谁负责”的要求，强化自律，积极主动地做好信息安全工作。要落实信息安全责任制，指定专人负责信息安全监管，成立专门的信息安全保障工作组，并与相关管理部门建立机制和确定联系人员，确保有关管理部门能及时与经营者取得联系，处理网上出现的有害信息传播行为。

二、互联网信息服务提供者要严格遵守《互联网信息服务管理办法》等有关法规规定，不得制作、复制、发布、传播国家规定的“九不准”有害信息。

互联网信息服务提供者发现其网站传输的信息明显属于国家规定的“九不准”有害信息的，应立即删除，保存有关记录，并同时向国家有关机关报告。

三、提供电子公告服务的互联网信息服务提供者，要严格遵守《互联网电子公告服务管理规定》（信息产业部令第3号）等有关规定，并重点做好以下工作：

（一）严格执行栏目明确制度，按照批准或者备案的类别和栏目提供服务，不得超出类别或另设栏目提供服务。

（二）进一步明确和强调版主负责制度，对获准的各个栏目制定不少于一名的专职人员充当版主，明确版主应承担对版内内容进行人工过滤、筛选和监控等管理职责，一旦发现违规内容，有关主管部门将追究网站和有关版主的责任并依法予以处理。

（三）严格执行规则张贴制度，在用户点击访问时弹出载有电子公告服务规则的页面，提示其发布信息所可能承担的法律責任。

（四）坚持对用户帖文上网实行先审后发制度。进一步强化技术保障措施和手段，对用户发出的信息预先进行软件自动过滤和人工过

滤，然后供人浏览，不得未经审查直接上网公开。

（五）严格落实记录保存制度，应当记录所提供的电子公告信息内容及其发布时间、互联网地址。

四、提供即时通信软件群组功能的互联网信息服务提供者，要进一步强化信息安全保障的技术措施和管理制度，并重点做好以下工作：

（一）进一步加强对群组创建和加入的管理，不允许出现含有有害信息的群组名称，新成员入群时必须经过群创建者的认可。

（二）在成员进入群组时，提示其发布信息所可能承担的法律責任，对成员发布信息的行为做出应服务有关法律规定和政府要求的警示和限定。

（三）严格控制群组成员数量上限。

（四）加强群组有害信息过滤、筛选工作。

五、网站接入服务提供者（包括互联网接入服务业务经营者、因特网数据中心业务经营者以及以其他方式为网站提供接入服务的电信业务经营者）要切实承担起相应的监督和配合查处责任，并重点做好以下工作：

（一）进一步强化对网站许可或备案证明的核验工作，不得为未经许可或备案的网站提供互联网接入服务。

（二）依照国家有关规定做好所接入用户信息动态管理、记录留存、有害信息报告等网络信息安全管理的工作，根据有关部门的要求对所接入用户进行监督。

（三）对有关主管部门依法处以关闭处罚的网站，应当立即终止为其提供网站接入服务。

广东省通信管理局 广东省公安厅

2005年4月20日

6. 浙江省《关于促进网络市场快速有序发展的若干意见》

各市、县（市、区）工商行政管理局：

2012年省政府出台《关于进一步推进商品交易市场提升发展的意见》（浙政发〔2012〕65号）文件，提出通过两个珠联璧合，即市场和实业的珠联璧合，实体市场和网络市场的珠联璧合，争取实现实体市场和网络市场成交额各达到2万亿元的目标。为全面贯彻落实省政府文件精神，着力推进全省网络市场快速有序发展，再创浙江市场新辉煌，现就加快我省网络市场健康有序发展特提出如下贯彻意见：

一、大力支持和扶持我省网络市场健康有序发展

围绕通过三到五年的努力，实现全省网络市场250家，网络市场成交额达到2万亿元的这一总体目标，全省工商部门要积极发挥职能作用，通过各种途径，大力支持和扶持网络市场健康有序的发展。要鼓励网络市场通过建设电子商务园区、物流体系等多种途径，强化与地方经济的联系，实现网络市场与全省产业、企业、实体市场的融合创新，充分发挥网络市场对拓展浙江产品市场、提升浙江企业品牌、创造就业机会、推动浙江产业乃至经济社会转型升级等方面的战略性功能，从而实现浙江经济新的竞争优势。

二、便捷市场准入，大力培育网络市场主体发展

（一）支持企业名称体现网络经济特征。鼓励网络市场主体名称体现行业特点，允许使用“电子商务”或表明其行业特点的各类新兴行业用语作为行业表述。在不违反企业名称登记管理相关规定的前提下，电子商务企业可以使用包括自有网站中文域名在内的个性化词语作为企业名称的字号（商号）。

（二）放宽经营场地限制。国家和地方政府批准设立的科技产业园区内设立的企业，可以凭园区管委会出具的住所使用证明，办理注册登记手续。

（三）放宽电子商务企业等新兴网络行业的经营范围。电子商务企业可以使用“网上经营××”或“网上提供××服务”等作为经营范围。对《国民经济行业分类》未包含的新兴网络经济行业，登记机关可以根据企业申请，参照《新兴行业企业登记试行意见》（企函字〔2012〕4号）的规定，依法灵活核定其经营范围。

（四）支持电子商务企业做大做强。鼓励符合条件的电子商务企业申报无区域企业名称。取冠“浙江”字样的电子商务企业，企业注册资本最低限额可以分期出资。电子商务企业组建集团的，母公司注册资本放宽到1000万元，子公司数量放宽到3个，母子公司注册资本放宽到3000万元。

（五）免征网络市场主体登记费。自2013年1月1日至2014年12月31日，免征各类网络市场主体注册登记费。

三、积极支持网络市场冠省名

要积极支持网络市场冠省名。对网络市场登记后运行正常，交易管理制度健全，交易服务体系齐全，交易规模大，辐射面广，年成交额10亿元以上，信用记录良好的网络市场，可以申请冠省名。

四、积极支持网络市场申报省星级文明规范市场和省重点市场

要根据全省网络市场发展状况，从支持和扶持网络市场发展的目标出发，修订浙江省星级文明规范市场、省重点市场的考核标准，制订网络市场的省四星级、五星级文明规范市场标准，积极支持网络市场申报省星级文明市场和省重点市场。

五、积极支持网络市场培育和创建自主品牌

推进网络市场实施商标战略，支持和鼓励网络市场和网店经营者申请注册商标，创立自主品牌。对于具有自主品牌、良好产品质量、较高市场信誉的网络市场和网店经营者，要建立品牌培育库，实施重点扶持、梯级培育，鼓励其争创浙江省著名商标、驰名商标。支持有

条件的网络市场建立品牌指导站，加强品牌的服务、指导和管理，促进网络市场的品牌培育和发展。

六、大力推进网络市场与实体市场的有机对接

要着力培育“网络与实体，网上与网下融合、互补的市场”，鼓励传统商品交易市场特别是小商品、轻纺产品、五金电子、皮革服装等集散型专业市场，不断提升信息化水平，积极发展网上交易平台，建立网上公共交易和服务平台。帮助广大市场经营户设立网上商铺，发布信息、展示商品、洽谈交易，促进网下店铺与网上店铺的有机结合，利用两种业态拓展国内外市场。同时，还要充分发挥我省电子商务先发优势，营造全国最具竞争力的电子商务发展环境。要引导现有的电子商务企业做大做强，创新交易模式，加快商品流通，降低交易成本，提高物流速度和信息化水平，实现与实体市场的有机对接。通过网络市场与实体市场的合作开发、错位发展，实现我省网络市场与实体市场的发展优势互补，从而建立我省市场形态多元化、交易方式多样化的现代商品交易市场体系。

七、建立健全网络市场维权机制

要建立网络市场打假维权联络员制度，加强工商与网络市场打假维权联络员间、工商与网站间的信息交流和指导服务，及时受理公众举报投诉，并接受社会的监督。有条件的网络市场要设立消费维权预赔基金制度，切实维护消费者合法权益。同时要严厉打击利用网络经营假冒伪劣商品、开展不正当竞争行为、侵害消费者权益和从事非法传销等违法行为，切实维护网络市场秩序。

八、加强网络市场信用体系建设

（一）以工商信用监管为基础，建立网络市场信用监管体系。建立经营者信用监管档案，实施信用监管评价，完善分类监管制度，建立网上巡查和实地检查相结合的监管机制。

（二）加强信用指导，建立健全网络信用投诉处理机制、违法失

信行为查处机制、交易者黑名单禁入机制，营造良好的网络信用环境。

（三）做好网络市场各项信用资产的开发、培育、使用和管理工作。引导浙江企业优先到信用好的网络市场开展电子商务业务。对信用监管评价等级 AAA、AA 级的经营者，实行重点走访制度，帮助其获取更多信用资产。

（四）引导网络市场举办者健全信用管理体系，建立交易者信用档案，提供科学、公平的信用评估服务，全面实施信用警示、信用披露和信用保障等制度。

（五）鼓励信用管理规范的网络市场探索供应链金融，为其经营者提供金融支撑。

（六）深化数字证书应用，积极为经营者提供网上亮照、网上金融账户年检、在线授权信用查询服务、企业网上身份认证等应用服务。

九、积极培育网络广告产业，规范网络广告经营行为

要积极培育我省网络广告产业的发展，大力扶持网络市场举办者依法开展网络广告代理、发布等业务，鼓励广告主通过发布网络广告，宣传自身形象，提升自身产品或服务的知名度。同时要充分发挥国家互联网广告监测中心落户浙江的优势，加强对网络广告发布的实时监测，严肃查处网络广告违法行为，规范网络广告经营秩序。

十、积极支持各级网商协会发展，加强行业自律

支持网络市场举办者和网商组建网商协会等行业自律组织，制定行业自律规范，建立行业自我教育、自我管理和自我服务的工作机制，充分发挥行业协会在宣传和执行国家法律政策、维护社会稳定、提供优质服务、培育专业和维护行业权益等方面的积极作用，推动我省网络市场行业的健康快速发展。

浙江省工商行政管理局

2013 年 5 月 17 日

7. 《浙江省信息化促进条例》

（涉及电子商务、电子政务推广方面）

第四章 信息技术推广应用

第二十四条 县级以上人民政府信息化主管部门应当根据本行政区域信息化发展规划，组织制定信息技术推广应用计划，确定推广应用目标和重点领域，落实推广应用措施。

县级以上人民政府及有关部门应当采取措施，鼓励和引导物联网技术的研究和推广应用。

第二十五条 县级以上人民政府及有关部门应当根据本行政区域电子政务规划，建立健全电子政务网络服务体系，充分依托电子政务网络完善政府信息查询系统，依法公开政府信息，办理行政管理和公共服务事项，提高行政效能。

第二十六条 县级以上人民政府信息化、通信管理、广播电视、文化、公安、工商行政管理和教育等部门应当利用信息技术加强对网络传播媒体、互联网上网服务营业场所和网络文化产品的管理，杜绝淫秽色情、暴力犯罪等有害信息的传播，建设文明健康的网络文化。

第二十七条 县级以上人民政府及有关部门应当推进信息技术在城镇管理中的应用，整合共享与交通、治安、市容环卫、突发事件应急处置等有关视频监控系统，提高城镇综合管理水平。

第二十八条 县级以上人民政府及有关部门应当完善农村信息化基础设施，建立农村综合信息服务体系，加强对农村的信息服务和指导，推广信息技术在农业生产、农村社会管理、农村文化生活等方面的应用，促进城乡一体化发展。

第二十九条 县级以上人民政府信息化主管部门应当会同有关部门加强对集成电路卡推广应用的指导，根据需要推进集成电路卡在交

通、医疗、社会保障、文化等领域的一卡多用，提高社会公共服务水平。

第三十条 供水、供电、供气、电信、电视、公共交通等公用企业事业单位，应当建立健全信息服务体系，通过信息化手段开展相关的业务申请、信息查询、费用支付、预约登记等业务办理工作。

第三十一条 鼓励和引导企业加大信息技术在设计研发、生产装备、生产过程、经营管理等方面的应用力度，提高生产和管理效能。

第三十二条 鼓励企业和个人应用信息技术依法从事商务活动，推进电子商务、电子金融、网络增值等服务业的发展。

电子商务服务提供商应当建立健全网商登记信息审核、网上商品和服务信息发布、交易行为管理、交易信用评价、用户及交易信息保密、信息安全保障、投诉处理等制度。

（涉及电子信息采集方面）

第五章 信息资源开发利用

第三十三条 各级人民政府及有关部门应当依法、及时、有序采集政府信息，建立政府信息更新和信息资源管理制度，确保信息的真实、准确、完整和安全。

具有保存利用价值的电子文件应当按照档案管理要求及时归档、登记备份。

第三十四条 县级以上人民政府及有关部门应当按照国家和省有关规定，建立和完善人口、法人单位、自然资源与地理空间、宏观经济等基础信息资源库。

县级以上人民政府有关部门和公用企业事业单位应当按照规定采集、分析、加工各类业务信息，建立本部门（系统）的业务信息资源库和应用服务系统。

除涉及国家秘密或者法律、法规另有规定外，基础信息资源库和业务信息资源库的建设或者管理单位应当按照规定为社会提供信息共享服务。

鼓励企业、其他组织和个人依法利用基础信息资源和业务信息资源进行公益性或者经营性的增值开发。

第三十五条 县级以上人民政府应当建立政府信息交换平台，完善信息资源交换机制和制度，通过电子政务网络实现信息资源共享和业务协同。

有关部门和公用企业事业单位应当依法、及时向本级政府信息交换平台提供本部门、本单位相关信息。

第三十六条 县级以上人民政府应当制定信息资源开发利用的相关政策，建立健全网络信息市场秩序，引导信息商品的流通和消费，促进信息的有效利用。

第三十七条 任何单位和个人不得利用网络与信息系统从事危害国家安全，损害国家利益、社会公共利益以及公民、法人或者其他组织合法权益的活动，不得制作、复制、发布、传播含有法律、法规禁止内容的信息。

第三十八条 金融、保险、电信、供水、供电、供气、医院、物业、房产中介以及其他掌握公众信息的单位，不得将其在提供服务过程中获得的公民、法人和其他组织的信息出售或者以其他方式非法提供他人。

任何单位和个人不得非法获取公民、法人和其他组织的信息。

第六章 信息安全保障

第三十九条 县级以上人民政府信息化主管部门应当会同公安、

国家安全、保密、密码管理、通信管理等部门，加强信息安全管理，建立健全相应的协调机制和应急处置机制，完善信息安全保障体系。

第四十条 网络与信息系统的主管部门和运营、使用单位，应当建立信息安全保障工作责任制和信息安全管理制度，落实信息安全保护措施，保证网络与信息系统的运行。

第四十一条 网络与信息系统的建设和运营、使用单位，应当按照国家和省有关信息安全等级保护的规定，确定本单位网络与信息系统的等级，按照规定进行定级评审、备案和相应的信息安全等级测评，并同步开展信息系统安全建设或者改建工作；其信息系统应当使用符合法律、法规和国家有关技术标准的信息系统安全专用产品。

第四十二条 基础网络和重要信息系统的运营、使用单位，应当按照国家技术规范和标准，进行信息安全风险评估，或者委托具有相应资质的检测机构进行评估，并根据评估结果，采取相应的安全保护措施。

县级以上人民政府信息化主管部门应当组织有关部门对基础网络和重要信息系统的信息安全进行检查；必要时，可以组织有关部门进行信息安全风险检查评估。

基础网络和重要信息系统的范围，由省信息化主管部门确定，并报省人民政府批准。

第四十三条 基础网络和重要信息系统的运营、使用单位，应当按照国家和省有关规定建立健全容灾备份系统和灾难恢复机制，确保信息安全和作业的连续性。

第四十四条 县级以上人民政府信息化主管部门应当会同有关部门编制本行政区域网络与信息安全突发事件应急预案，经本级人民政府批准后实施，并报上一级信息化主管部门备案。

基础网络和重要信息系统的主管部门和运营、使用单位，应当按照国家和省有关规定制定网络与信息安全突发事件应急预案，定期演练。应急预案应当按照规定报信息化主管部门及有关部门备案。

发生网络与信息安全突发事件时，事发单位应当迅速启动应急响应，及时采取措施，防止事件扩大，保存相关记录，按照规定向本级人民政府和有关部门报告；县级以上人民政府及有关部门应当按照应急预案的规定，开展应急处置。

第四十五条 任何单位和个人不得擅自拆除、迁移或者损毁电信网、广播电视网、互联网等公共信息基础设施；不得从事故意制作、传播计算机病毒等危害网络与信息安全的活动。

8. 《湖南省信息化条例》

（涉及个人电子信息采集方面）

第三章 信息资源开发利用

第十七条 县级以上人民政府及其有关部门应当建立信息资源开发利用保障机制，建立和完善本行政区域的基础信息共享平台，促进政务信息资源共享和信息资源社会化开发利用。

第十八条 县级以上人民政府信息化主管部门应当会同有关部门制定政务信息资源目录，完善交换共享体系，组织有关部门共同推进重大基础性信息资源的开发利用，推动政务信息在国家机关之间的资源共享和利用。

第十九条 国家机关采集信息，应当遵循一个数据一个来源的原则，并在其职责范围内做好信息资源维护、更新、管理，避免重复采集、多头采集。

国家机关在履行职责过程中形成或者获取的信息资源应当依照相

关规定予以共享。

第二十条 国家机关以外的单位和个人向公民、法人和其他组织采集信息，应当征得被采集人同意，说明用途，并在该用途范围内使用所采集的信息。

第二十一条 任何单位和个人不得违反国家规定，非法披露所采集的信息，将获取的公民、法人和其他组织的信息出售或者以其他方式非法提供他人，以窃取等方式非法获取信息。

第二十二条 信息资源开发利用应当依法保护国家秘密、知识产权、商业秘密和个人隐私。

信息服务提供者发布的信息应当合法、真实，不得制作、复制、发布、传播含有法律、法规禁止内容的信息。

公民、法人和其他组织有权要求采集、使用其信息的单位和个人更正、删除与其相关的不实信息。

第二十三条 县级以上人民政府应当支持重点领域公益性信息资源的开发利用，引导公民、法人和其他组织开发信息资源，开展公益性信息服务。

鼓励和支持信用服务机构依法采集、整合信用信息，为社会提供信用征信、评估评级、信用管理等服务。

第二十四条 县级以上人民政府应当推动信息资源开发利用市场化，鼓励政府部门采用外包、政府采购等方式获取信息服务。

第四章 信息技术推广应用

第二十五条 县级以上人民政府信息化主管部门应当组织编制本地区信息技术推广应用指南，确定推广应用目标和重点领域，完善推广应用体系，实行引进推广应用先进成果和自主创新相结合，组织实

施重点推广应用项目。

科技、技术改造、农业发展等专项资金应当安排一定比例用于引导和扶持相关领域信息技术的推广应用。

第二十六条 县级以上人民政府应当推进信息化与工业化融合，推动信息技术在设计研发、生产装备、生产过程以及经营管理等方面的应用；支持应用信息技术改造传统产业，促进产业转型升级；建设面向中小企业的公共信息服务平台，支持中小企业应用信息技术。

第二十七条 各级人民政府和县级以上人民政府有关部门应当加强对农村的信息服务和指导，推进农村现代远程教育；推广信息技术在农业生产与经营、农村社会管理、农村文化生活等方面的应用；鼓励通过信息化手段为农民提供生产、生活应用信息服务，发挥农村专业合作社等作用，开发、利用农村信息资源，开展面向农民的信息化知识和技能培训。

第二十八条 省人民政府推进建立全省统一的电子政务网络；县级以上人民政府应当建设统一的电子政务平台。

国家机关建设电子政务工程应当充分利用已有电子政务平台，实现互联互通，推进信息技术在社会管理和公共服务等方面的应用，促进政务资源共享和业务协同，提高行政效能和公共服务水平。

第二十九条 县级以上人民政府有关部门和社会公共服务机构，应当建立健全社会管理信息网络，及时、准确提供与民众生活相关的公共信息服务。

鼓励整合社区公共服务信息资源，构建社区综合便民服务平台，提高社区公共服务水平。

第三十条 县级以上人民政府应当支持建立和完善社会信用服务、安全认证、在线支付和现代物流等支撑体系，推动电子商务建设和应用，

促进电子商务发展。

第三十一条 机关、团体、企业事业单位应当根据自身特点，加大信息化投入，加强信息化建设和管理，提高信息化水平，推进信息技术在工作、生产、经营中的应用。

第五章 信息产业发展

第三十二条 县级以上人民政府应当根据本行政区域信息化的需要，制定鼓励信息产业发展的优惠政策；支持信息产业基地建设，推动信息技术创新和应用，引导信息产业发展。

鼓励建立产学研用合作机制，联合研究、开发、推广信息技术产品和服务，推进创新成果的产业化。

第三十三条 省人民政府信息化主管部门应当会同有关部门编制信息产业发展目录，定期公布信息产业关键技术和产品指南。

第三十四条 从事信息技术产品制造、软件开发和信息服务的企业应当遵守诚实信用的原则，为用户提供优质的产品和服务，不得损害用户和其他经营者的合法权益；并按照国家标准、行业标准、地方标准和有关规范的要求，组织产品生产和技术开发。

从事信息技术产品制造、软件开发以及信息服务的企业，按照国家 and 省有关规定享受税收减免、投资融资、土地使用、人才培养等方面优惠政策。

第三十五条 设计、制造电子产品，应当采用节约资源、保护环境的材料、技术和工艺。

鼓励采用先进工艺集中处理废弃电子产品。

第三十六条 电子交易服务提供商应当对利用其电子交易平台从事经营活动的经营主体的身份信息、合法经营凭证和反映交易信用状

况的材料进行核查，并对相关信息做好数据备份，便于当事人和有关部门查询、核对。

电子交易服务提供商应当建立投诉受理机制，对利用其电子交易平台从事的经营活动进行监督，配合政府有关部门的管理活动，但不得妨碍相关经营主体开展正常交易活动。

电子交易服务提供商应当对利用其电子交易平台从事交易活动的信息采取安全保密措施，未经当事人同意，不得向他人泄露或者出售。

第三十七条 信息终端维修、维护服务的提供者对其维修、维护的信息终端储存的信息，不得复制、泄露和出售。

第三十八条 建立信息化人才培养和引进机制，普及中小学信息技术教育，发展信息技术职业教育。

第三十九条 鼓励信息产业行业协会和有关社会中介组织按照诚信、守法的原则，依法开展信息市场调查、信息交流、咨询和评估等中介活动，加强行业自律。

第六章 信息安全保障

第四十条 县级以上人民政府应当加强信息安全基础设施建设，建立和完善信息安全保障体系，提高信息安全防御能力。

第四十一条 县级以上人民政府信息化主管部门应当会同有关部门和机构，加强信息安全协调管理，建立健全信息安全等级保护、安全预警、风险评估、应急指挥、安全通报和责任认定制度。

第四十二条 县级以上人民政府信息化主管部门应当会同有关部门推动信息安全技术的研发和产业化，在电子政务、电子商务和公共服务等领域推广应用电子签名，采用自主可控的信息安全产品和服务。

第四十三条 信息网络和信息系统的主管单位或者运行单位应当

根据国家有关规定，确定本单位信息网络和信息系统的等级，并进行相应的信息安全系统建设。

信息安全系统必须采用依法认证的信息安全产品，并与信息网络和信息系统同时设计、同时施工、同时投入使用。

第四十四条 关系国计民生、社会稳定的基础信息网络和重要的信息系统应当进行信息安全测评和风险评估，建设容灾备份系统。对涉及国家秘密的信息网络和信息系统应当按照国家有关保密规定做好信息保密工作。

第四十五条 信息网络与信息系统的单位或者运行单位，应当确定信息安全管理人，建立信息的安全管理制度，加强信息安全教育，保证本单位信息网络与信息系统的安全运行。

基础信息网络和重要信息系统的所属单位或者运行维护单位应当制定信息安全事件应急预案，并报相关主管部门备案。

发生信息网络或者信息系统安全事件，其所属单位或者运行单位应当迅速采取措施降低损害，防止事态扩大，保存相关记录，并按照规定及时向相关主管部门报告。

第七章 监督管理

第四十六条 县级以上人民政府信息化主管部门应当会同有关部门，对信息化发展规划实施情况、使用财政性资金的信息工程建设情况、信息化标准执行情况等进行监督检查。

县级以上人民政府信息化主管部门应当建立健全信息服务市场管理制度，加强对信息服务市场的监督管理，维护信息服务市场秩序。

第四十七条 县级以上人民政府公安机关负责信息系统安全等级保护工作的监督检查，依法查处破坏信息基础设施、危害信息安全、

扰乱社会秩序的违法行为。

县级以上人民政府国家安全机关负责信息系统国家安全工作的监督检查及涉及国家安全的信息网络的反窃密技术安全工作，依法查处利用网络信息危害国家安全的违法行为。

县级以上人民政府保密、密码管理等机构分别负责信息系统保密、密码工作的监督检查。

第四十八条 县级以上人民政府广播电视部门和通信管理机构应当加强对基础信息网络的监督管理，防止利用网络信息危害国家安全、扰乱社会秩序，危害公民、法人或者其他组织的合法权益。

第四十九条 县级以上人民政府有关部门应当组织对本系统公共服务机构的公共信息服务情况进行监督检查，并将有关情况向社会公布。

第五十条 县级以上人民政府财政部门应当会同信息化主管部门及其他有关部门加强信息资产的监督管理，建立信息资产评估制度，促进信息资源的优化配置。

县级以上人民政府审计机关应当加强对使用财政性资金建设的信息工程项目的审计监督。

9. 《江苏省信息化条例》

（涉及个人电子信息采集方面）

第三章 信息资源共享与开发利用

第二十条 县级以上地方人民政府应当建立信息资源开发利用保障机制，建设和完善本行政区域内的人口、法人、自然资源和空间地理、宏观经济、信用征信等基础信息共享平台，促进政务信息资源共享和

信息资源社会化开发利用。

第二十一条 省人民政府信息化主管部门应当会同有关部门在本行政区域内建立统一规范的政务信息资源共享目录和共享交换体系，推动政务信息在国家机关之间的资源共享和充分利用。

设区的市、县（市）人民政府信息化主管部门应当会同有关部门建立相应的政务信息资源共享目录和共享交换体系。

第二十二条 国家机关应当遵循一个数据一个来源和谁采集、谁更新、谁负责的原则，在各自职责范围内做好信息资源采集、维护、更新，不得重复采集、多头采集。

国家机关在履行职责过程中形成或者获取的信息资源应当依照相关规定予以共享。

第二十三条 国家机关以外的单位和个人向公民、法人和其他组织采集信息，应当征得被采集人同意，并说明用途。

信息采集人应当在向被采集人说明的用途范围内使用所采集的信息。

第二十四条 任何单位和个人不得非法披露所采集的信息，不得将获取的公民、法人和其他组织的信息出售或者以其他方式非法提供给他人，不得以窃取、购买等方式非法获取上述信息。

第二十五条 信息资源开发利用应当依法保护国家秘密、知识产权、商业秘密和个人隐私。

信息服务提供者发布的信息应当合法、真实，不得制作、复制、发布、传播含有法律、法规禁止内容的信息。

公民、法人和其他组织有权要求采集、使用其信息的单位和个人更正、删除与其相关的不实信息。

第二十六条 引导和鼓励公民、法人和其他组织开发信息资源，开展公益性信息服务。

鼓励和支持信用服务机构依法采集、整合信用信息，为社会提供信用征信、评估评级、信用管理等服务。

鼓励在政府采购、市场监管、招标投标、信贷等活动中使用信用服务机构提供的信用服务。

第四章 信息产业发展与技术推广应用

第二十七条 省人民政府信息化主管部门应当会同有关部门适时编制、发布本省信息技术推广应用指南，确定信息产业发展重点领域。

第二十八条 县级以上地方人民政府应当结合本地实际，优先发展新一代信息技术产业，制定鼓励信息产业发展的优惠政策和措施。

从事电子信息产品制造、软件开发、信息服务的单位，按照国家和省有关规定，享受优惠政策。

第二十九条 县级以上地方人民政府及其信息化主管部门应当鼓励和支持信息产业中介组织开展市场调查、信息交流、企业合作、咨询评估等活动。

第三十条 县级以上地方人民政府及其有关部门应当采取有效措施，促进信息化和工业化融合发展，加快信息技术在区域、行业、企业的示范应用，推进产业转型和发展方式转变。

县级以上地方人民政府及其有关部门应当推动建设公共技术服务平台和信息技术应用服务平台，引导和鼓励企业在生产、经营、管理中广泛应用信息技术，促进技术进步和产业升级。

县级以上地方人民政府及其有关部门应当制定以中小企业为主的企业信息化应用发展指南，建设面向中小企业的公共信息服务平台，

支持和扶持中小企业应用信息技术。

第三十一条 省人民政府推进建立全省统一的电子政务网络。县级以上地方人民政府应当建设统一的电子政务平台。国家机关建设电子政务工程应当充分利用已有电子政务平台，实现互联互通。

县级以上地方人民政府及其有关部门应当应用信息与网络技术，向社会提供公共管理与服务，依法履行下列职责：

- （一）利用政府网站及时、准确公开政府信息；
- （二）推行政府公共管理和公共服务事项在线办理；
- （三）组织对公务人员的信息化知识培训、考核。

第三十二条 县级以上地方人民政府应当推广应用电子签名，建立和完善社会信用、在线支付、物流配送等多种服务体系，促进电子商务的发展。

第三十三条 县级以上地方人民政府应当统筹城乡信息化发展，支持农村信息基础设施和农村综合信息服务平台建设及运行维护，鼓励开发、利用涉农信息资源，通过多种信息化手段为农民提供市场、科技、政策法规等信息服务。

第三十四条 县级以上地方人民政府应当加强社区信息服务体系建设，推进居民自助、互助、无线、远程等信息便民服务设施的建设，整合各类资源和业务，构建统一的社区管理和综合信息平台。

省、设区的市、县（市）人民政府应当推进公用事业智能卡跨行业和跨地区使用。

第三十五条 教育、科技、社会保障、环境保护、交通运输、文化、卫生、人口计生、广播电视、新闻出版、气象等有关部门或者机构以及供电、供水、供气、金融、保险等单位，应当应用信息技术，及时、准确提供与民众生活相关的公共信息服务。

第五章 信息安全保障

第三十六条 县级以上地方人民政府应当加强信息安全保障体系建设，建立健全信息安全等级保护、信息安全风险评估和政务信息网络与信息系统安全检查制度，提高政务信息网络与信息系统的安全风险防御能力和处理信息安全突发事件的能力。

信息化主管部门具体负责统筹推进信息安全保障体系建设和信息安全风险评估，会同有关部门负责政务信息网络与信息系统安全检查和信息安全突发事件应急处置等工作。

公安部门负责信息安全等级保护工作的监督、检查和指导。

公共基础信息网络主管部门具体负责公共基础信息网络的信息安全等级保护、风险评估和突发事件应急处置等工作。

涉及国家安全、国家秘密的信息系统安全等级保护，按照国家有关规定执行。

第三十七条 信息网络和信息系统的所属单位或者运行维护单位应当依据国家有关规定以及相关技术标准，建立信息安全保障工作责任制，制定本单位信息安全保护和容灾备份措施，对信息网络和信息系统实行信息安全等级保护，定期进行信息安全风险评估。

第三十八条 从事安全运行维护管理、风险评估、等级保护等信息安全专业服务活动的，应当符合国家和省的有关规定，接受所在地相关主管部门监督。

第三十九条 信息安全保障系统应当与信息化工程项目同步规划、同步建设、同步运行。使用财政性资金建设的信息网络和信息系统投入使用前，应当进行信息安全等级保护和信息安全风险评估。

信息网络和信息系统的建设及其运行维护，应当选择依法取得认证认可的信息安全产品和服务。

第四十条 基础信息网络和重要信息系统的所属单位或者运行维护单位应当制定信息安全事件应急预案，向相关主管部门备案，并由相关主管部门进行效能评估。

发生信息网络或者信息系统安全事件，所属单位或者运行维护单位应当迅速采取措施降低损害，防止事态扩大，保存相关记录，并按照规定及时向相关主管部门报告。

10. 《海南省信息化条例》

（涉及个人电子信息采集方面）

第三章 信息资源开发利用与技术推广

第二十条 省人民政府应当建立全省统一的电子政务公共平台。

国家机关应当依托全省统一的电子政务公共平台建设电子政务工程，不得新建专用网络。非涉及国家秘密的政务信息化业务系统应当建设在省政务外网平台上。国家和本省另有规定的除外。

国家机关应当依托电子政务公共平台开展政务公开和政务服务。按照法律法规规定属于主动公开的政务信息，应当在该信息形成或者变更之日起二十个工作日内予以公开。法律法规对政府信息公开的期限另有规定的，从其规定。

第二十一条 省人民政府信息化主管部门会同有关部门依托全省统一的电子政务公共平台，建立电子政务信息共享交换平台，实现国家机关内部基础信息资源共享和业务协同。

省人民政府应当利用信息共享交换平台，集中建设和完善地理、人口、法人等基础数据库，以及工商、税收、文化、教育、医疗、社会保障、质监等业务数据库。

国家机关应当准确、完整、无偿、及时地向信息共享交换平台提供本部门、本单位的相关信息。

第二十二条 国家机关应当按照谁采集、谁更新、谁负责的原则，在各自职责范围内做好信息资源采集工作，不得重复采集，多头采集。

国家机关以外的单位和个人向公民、法人或其他组织采集信息，应当征得被采集人同意，说明用途，并在该用途范围内使用所采集的信息。

单位和个人采集利用信息，应当依法保护国家秘密、知识产权、商业秘密和公民个人电子信息。

第二十三条 省人民政府应当加强生态环境保护综合信息平台建设，推进生态环境保护的自动监控、应急等信息系统建设，提升重点污染源的监管能力。

第二十四条 省人民政府应当加强旅游综合信息服务平台建设，发展旅游电子商务、推进旅游信息基础设施建设、为游客提供全方位的旅游信息服务。

省人民政府旅游主管部门会同有关部门建立统一的旅游基础信息资源标准数据规范与共享机制，鼓励智能终端、物联网、移动通信等信息技术在旅游各环节的应用服务，提升旅游管理信息化水平。

第二十五条 省人民政府应当加强农业综合信息服务平台建设，提供生产销售、科技信息、技术推广、市场信息、农村金融等服务。建立健全农产品质量安全信息监督管理体系，保障农产品质量安全。

第二十六条 省人民政府应当加强海洋信息业务网和海洋环境与基础地理信息服务平台建设，推动信息技术在我省海洋渔业生产、海洋测绘、海域监视等领域的广泛深入应用，提升海洋产业信息化水平。

第二十七条 县级以上人民政府信息化主管部门应当组织编制本

地区信息技术推广应用指南，确定推广应用目标和重点领域，完善推广应用体系，实行引进推广应用先进成果和自主创新相结合，组织实施重点推广应用项目。

第二十八条 县级以上人民政府应当推进信息化与工业化融合，推动信息技术在设计研发、生产装备、生产过程以及经营管理等方面的应用，支持应用信息技术改造传统产业，促进产业转型升级。

第二十九条 县级以上人民政府应当推动建立和完善安全、信用、金融、物流和标准等支撑体系，引导电子商务平台向提供涵盖信息流、物流、资金流的全流程服务发展，推动电子商务建设和应用。

第三十条 县级以上人民政府应当加强社区信息服务体系建设，推进信息便民服务设施建设，整合各类资源和业务，构建统一的社区管理和信息服务信息平台。

省人民政府信息化主管部门应当会同有关部门加强对集成电路卡推广应用的指导，推进集成电路卡在交通、医疗、社会保障、金融等领域的一卡多用。

11. 《山西省信息化促进条例》

（涉及个人电子信息采集方面）

第三章 信息资源共享与开发利用

第十六条 县级以上人民政府应当建立和完善本行政区域的人口、法人、自然资源与空间地理、宏观经济、文化等基础信息数据库，促进政务信息资源共享和信息资源社会化开发利用。

信息资源共享与开发利用的具体管理办法，由省人民政府制定。

第十七条 省信息化主管部门会同有关部门制定统一规范的政务信息资源的相关标准、共享目录，依托全省统一的电子政务网络和信

息资源共享交换平台，完善共享交换体系。

设区的市、县（市、区）人民政府及其有关部门编制本行政区域或者本单位信息共享目录，向信息资源共享交换平台提供相关信息，并依法向社会提供信息服务。

第十八条 国家机关应当遵循一个数据一个来源和谁采集、谁更新、谁负责的原则，在各自职责范围内做好信息资源采集、维护、更新，避免重复采集、多头采集。

国家机关以外的单位和个人采集信息，应当征得被采集人同意，说明信息的使用目的、方式和范围，不得违反法律、法规的规定和双方的约定收集、使用信息。

任何单位和个人不得非法获取信息，不得非法披露所采集的信息，不得非法出售或者以其他非法方式将获取的信息提供给他人。

第十九条 信息资源开发利用应当依法保护国家秘密、知识产权、商业秘密和个人隐私。

鼓励和支持对信息资源的公益性开发利用，引导和规范对信息资源的增值性开发利用。

鼓励和支持信用服务机构依法采集、整合信用信息，为社会提供信用征信、评估评级、信用管理等服务。

第二十条 公共服务机构和其他拥有公众信息的单位，应当采取措施，防止个人信息的泄露、篡改、毁损和丢失。

公民发现泄露个人身份、散布个人隐私等侵害其合法权益，或者受到商业性电子信息侵扰的，有权要求服务提供者删除有关信息或者采取其他必要措施予以制止，同时可以向公安机关举报。

公民、法人和其他组织有权要求采集、使用其信息的单位和个人更正、删除与其相关的不实信息。

12. 《辽宁省计算机信息系统安全管理条例》

第三章 信息安全和运行环境安全

第十九条 任何单位和个人不得利用信息系统制作、复制、发布和传播下列信息：

- (一) 反对宪法确定的基本原则的；
- (二) 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- (三) 损害国家荣誉和利益的；
- (四) 煽动民族仇恨、民族歧视，破坏民族团结的；
- (五) 破坏国家宗教政策，宣扬邪教、封建迷信的；
- (六) 散布谣言，煽动非法聚集，扰乱社会秩序，破坏社会稳定的；
- (七) 宣扬淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪，或者交易、制造违禁品、管制物品的；
- (八) 侮辱或者诽谤他人，侵害他人合法权益的；
- (九) 法律、法规禁止的其他内容。

第二十条 互联网服务提供者和联网使用单位应当建立信息审核制度，明确审核人员，发现本条例第十九条禁止的违法信息，应当先行保存有关记录，及时采取删除、停止传输等处置措施，并向公安机关等有关部门报告。

公安机关查处涉嫌违法犯罪行为时，互联网服务提供者和联网使用单位应当提供有关信息、资料、数据文件和原始记录。

第二十一条 任何单位和个人不得利用信息系统实施下列行为：

- (一) 未经允许侵入信息系统；

（二）非法获取、使用信息系统资源或者对信息系统实施非法控制；

（三）擅自向第三方公开他人电子邮箱地址和其他个人信息资料；

（四）窃取他人账号和密码，或者擅自向第三方公开他人账号和密码；

（五）未经允许，对计算机信息系统功能进行删除、修改、增加或者干扰；

（六）未经允许，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改或者增加；

（七）提供专门用于实施侵入、非法控制信息系统的程序、工具；

（八）故意制作、传播计算机病毒以及其他破坏性程序；

（九）其他危害信息系统安全的行为。

结 束 语

互联网的发展创新持续改变既有的法律规则，信息通信业的新立法主要集中在互联网领域。但互联网法律制度也不是全新的规则，传统立法也直接或通过修订适用于互联网，近年来，在很多立法修订中都增加了关于互联网的条款。

网络社会的发展，使人的权利延伸到网络空间，从而更易于受到侵害，如网络上的个人隐私保护、网络交易中的消费者保护、未成年人保护等问题突出；网络经济的发展，要求相对稳定的法律环境；网络文化的发展，使互联网内容空前繁荣，但是网络版权侵权问题突出。互联网的发展对法律制度带来了新的挑战，也使互联网成为立法最为活跃的领域。

互联网与传统行业的发展融合、互联网业务自身的融合，导致越来越多的传统行业主管部门进入互联网管理领域，立法主体增多，立法对象越来越复杂。技术业务的发展，产业价值和生产要素加速流向互联网，新兴业态蜂拥出现，云计算、大数据等的出现，使原有的法律规则面临新的挑战。

我国互联网法律制度建设受互联网与法律特性的内在矛盾和外部影响因素的共同作用。互联网的跨国性与法律适用的地域性之间的矛盾、互联网发展的快速性与法律的滞后性之间的矛盾、互联网的开放性与法律规范的原则性之间的矛盾，以及互联网的发展与管理目标的平衡是决定我国互联网法制建设的内在矛盾。国家管理互联网的意志、互联网管理的体制机制及相关国际规则是外部影响因素。

从国际上看，宽带的发展，使通信网络作为关键基础设施的地位加强，各国对关键信息基础设施加强立法；棱镜计划的曝光，使近几年一直有加强趋势的网络与信息安全立法显得更为重要；而云计算的发展和跨境数据流动的加速，使数据保护等问题超越了一国的管辖权范围，必将推动该领域的国际合作和国际规则的产生。

从国内看，2012年年底《全国人民代表大会常务委员会关于加强网络信息保护的决定》发布之后，相关配套立法是近几年立法的重点；随着电子商务的快速发展，关于网络购物消费者权益保护、用户信息保护、信用体系建设等亟须加以规范，电子商务将成为未来立法的重点领域；此外，随着《互联网信息服务管理办法》（修订版）的出台，互联网发展和管理也将进入崭新的阶段。

《中共中央关于全面深化改革若干重大问题的决定》指出，要“推进法治中国建设”，为我们描绘了法治中国的美好图景，我们有理由相信，未来的互联网发展将有更好的法制环境，互联网行业也一定拥有更美好的未来！

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为，歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010) 88254396；(010) 88258888

传 真：(010) 88254397

E-mail：dbqq@phei.com.cn

通信地址：北京市万寿路173信箱

电子工业出版社总编办公室

邮 编：100036